CA Access Control Premium Edition

엔터프라이즈 관리 안내서

r12.5

두 번째 버전

CA 제품 참조

이 문서는 다음 CA 제품을 참조합니다.

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On(CA SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management(CA NSM, 이전 이름: Unicenter NSM 및 Unicenter TNG)
- CA Software Delivery(이전 이름: Unicenter Software Delivery)
- CA Enterprise Log Manager
- CA Identity Manager

설명서 규칙

CA Access Control 설명서는 다음과 같은 규칙을 따릅니다.

형식	의미
고정 폭 글꼴	코드 또는 프로그램 출력
기울임꼴	강조 또는 새 용어
굵게	표시된 대로 동일하게 입력해야 하는 텍스트
슬래시(/)	UNIX 및 Windows 경로를 기술하는 데 사용되는 플랫폼 독립적인 디렉터리 구분 기호

이 설명서는 또한 명령 구문과 사용자 입력(고정 폭 글꼴로 표시됨)을 설명할 때 다음과 같은 특별한 규칙을 사용합니다.

형식	의미
기울임꼴	반드시 입력해야 하는 정보

형식	의미
대괄호([ ]) 사이	선택적 피연산자
중괄호({ }) 사이	필수 피연산자 집합
파이프(|)로 구분된 선택 사항	대체 피연산자(하나 선택)를 구분합니다. 예를 들어, 다음은 사용자 이름 또는 그룹 이름 중 하나라는 의미입니다. `{username|groupname}`
...	앞의 항목 또는 항목 그룹이 반복될 수 있음을 나타냅니다.
밑줄	기본값
줄 마지막에 공백 다음의 백슬래시(\)	때때로 이 안내서에서 명령이 한 줄에 모두 표시되지 않는 경우가 있습니다. 이런 경우에는 줄 끝에 공백과 백슬래시(\)를 표시하여 명령이 다음 줄에서 계속됨을 나타냅니다. **참고:** 실제 명령을 입력할 때는 이러한 백슬래시를 포함하지 말고 줄바꿈 없이 명령을 한 줄에 입력하십시오. 백슬래시 및 줄바꿈은 실제 명령 구문에 포함되지 않습니다.

예제: 명령 표기 규칙

다음 코드는 이 안내서에서 명령 규칙이 사용되는 방식을 보여 줍니다.

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

설명:

- 표시되는 그대로 입력해야 하는 명령 이름(ruler)은 일반 고정 폭 글꼴로 표시됩니다.
- className 옵션은 클래스 이름(예: USER)이 들어갈 자리이므로 기울임꼴로 표시됩니다.
- 대괄호로 묶인 두 번째 부분은 선택적 피연산자를 의미하므로 이 부분 없이 명령을 실행할 수도 있습니다.
- 옵션 매개 변수(props)를 사용할 때 키워드 all 을 선택하거나 하나 이상의 속성 이름을 쉼표로 구분하여 지정할 수 있습니다.

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 http://www.ca.com/worldwide에서 기술 지원팀에 문의하십시오.

설명서 변경 사항

두 번째 버전

이 설명서의 두 번째 버전은 r12.5 GA 때 제공되었습니다.

이 버전에서 다음 항목이 추가 또는 업데이트되었습니다.

- CA Access Control 엔터프라이즈 관리의 관리 역할(페이지 20) - 새 UNAB Administrator 관리 역할 및 여러 새 보고 관리 역할을 포함하여 항목이 업데이트되었습니다.
- 권한 있는 액세스 역할(페이지 23) - 권한 있는 액세스 역할을 사용자에게 할당할 때 고려해야 할 사항을 추가하여 항목이 업데이트되었습니다.
- 사용자를 관리 역할에 추가하는 방법(페이지 26) - 새 항목에서 관리 역할을 사용자에게 할당하는 프로세스에 대해 설명합니다.
- Active Directory 제한(페이지 32) - 새 항목에서 사용자 저장소로 Active Directory 를 사용하는 경우 수행할 수 없는 CA Access Control 엔터프라이즈 관리 작업에 대해 설명합니다.
- 문제 해결 정책 배포(페이지 86) - 복원 옵션에 대한 변경 사항을 추가하여 항목이 업데이트되었습니다.
- 권한 있는 계정 관리(페이지 95) - 권한 있는 액세스 역할이 사용자가 수행하는 PUPM 작업에 어떤 영향을 주는지 설명하기 위해 이 장의 많은 항목이 업데이트되었습니다. 또한 이 장의 항목에서 다음과 같은 내용이 변경되었습니다.
  - Windows Agentless 연결 정보(페이지 111) - WMI DYN Namespace 끝점 유형에 대한 새 이름으로 항목이 업데이트되었습니다.
  - SSH 장치 연결 정보(페이지 112) - SSH DYN Namespace 끝점 유형에 대한 새 이름으로 항목이 업데이트되었습니다.
  - SSH 장치 XML 파일 사용자 지정(페이지 113) - 새 항목에서 SSH 장치 XML 파일을 사용자 지정하는 방법에 대해 설명합니다.
- 권한 있는 계정 요청에 응답(페이지 130) - 사용자가 권한 있는 계정 요청에 응답해야 하는 요구 사항을 추가하여 항목이 업데이트되었습니다.

- UNAB 설정 방법(페이지 138) - "UNAB 의 작동 방법" 항목이 새 이름의 항목으로 대체되었습니다.
- UNAB 가 사용자를 인증하는 방법(페이지 138) - UNAB 가 사용자를 인증하는 방법에 대한 추가 정보로 항목이 업데이트되었습니다.
- 마이그레이션 충돌 해결(페이지 143) - UNAB 충돌 파일 출력의 예제를 추가하여 항목이 업데이트되었습니다.

첫 번째 버전

설명서의 첫 번째 버전은 r12.5 에서 제공되었습니다. 이 버전에서 설명서의 r12.0 SP1 릴리스에 다음 사항이 업데이트되었습니다.

- 소개(페이지 15) - 업데이트된 장에는 기본 엔터프라이즈 관리 기능에 대한 추가 정보가 수록되어 있습니다.
- CA Access Control 엔터프라이즈 관리 관리(페이지 19) - 이 장의 많은 항목은 인터페이스의 변경 사항을 반영하여 업데이트되었습니다.

  또한 이 장에는 다음과 같은 새 내용이 포함되어 있습니다.

  - 권한 있는 액세스 역할(페이지 23) - 새 항목은 권한 있는 액세스 역할을 설명합니다.
  - 관리 작업 만들기(페이지 29) - 새 항목은 관리 작업을 추가하는 방법을 설명합니다.
  - 그룹 유형(페이지 36) - 새 섹션은 인터페이스가 지원하는 그룹 유형을 설명합니다.
  - 감사 데이터(페이지 40) - 새 섹션은 CA Access Control 엔터프라이즈 관리가 제공하는 감사 기능을 설명합니다.
- 엔터프라이즈 구현 보기(페이지 47) - 업데이트된 장은 인터페이스에 대한 변경 사항과 추가된 새 기능을 반영합니다.
- 중앙에서 정책 관리(페이지 51) - 이 장의 많은 업데이트된 많은 장은 인터페이스에 대한 변경 사항을 반영하고 개념을 보다 구체적으로 설명합니다.

  또한 이 장에는 다음과 같은 새 내용이 포함되어 있습니다.

  - 정책 유형(페이지 51) - 새 항목은 CA Access Control r12.5 에서 사용할 수 있지만 고급 정책 관리를 사용하여 관리되지 않는 두 개의 추가 정책 유형을 설명합니다.
  - 배포 방법이 배포 작업에 주는 영향(페이지 54) - 새 항목은 배포 작업이 시작되는 방법을 설명합니다.

목차

제 4 장: 중앙에서 정책 관리 51

제 1 장: 소개

이 장은 아래의 주제를 포함하고 있습니다.

안내서 정보

이 안내서는 CA Access Control Premium Edition 의 엔터프라이즈 관리 및 보고 기능과 CA Access Control 엔터프라이즈 관리 웹 기반 인터페이스에 대한 정보를 제공합니다. CA Access Control 의 엔터프라이즈 관리 및 보고 기능에는 고급 정책 관리, 보고, 월드 뷰 엔터프라이즈 뷰어가 포함되어 있습니다.

용어를 간단히 나타내기 위해 이 안내서에서는 제품을 CA Access Control 이라고 합니다.

안내서 사용자

이 안내서는 다음과 같은 CA Access Control 의 엔터프라이즈 관리 및 보고 기능을 사용하려는 보안 및 시스템 관리자용으로 작성되었습니다.

- 엔터프라이즈 정책 관리
- 엔터프라이즈 보고
- 엔터프라이즈 호스트 액세스 관리 처리를 위한 웹 기반 인터페이스
- 권한 있는 사용자 암호 관리(PUPM)

엔터프라이즈 관리

CA Access Control 엔터프라이즈 관리는 회사 전체에서 액세스 관련 관리 작업을 수행할 수 있게 해주는 웹 기반 사용자 인터페이스입니다. CA Access Control 엔터프라이즈 관리를 사용하여 여러 관리 작업을 수행할 수 있습니다. 예를 들어, 중앙 위치에서 회사 전체에 액세스 정책을 배포하거나, 개별 호스트를 관리하거나, 권한 있는 계정을 관리하거나, 엔터프라이즈 보고서를 작성하는 등의 작업을 수행할 수 있습니다.

엔터프라이즈 관리 인터페이스

CA Access Control 엔터프라이즈 관리 인터페이스는 회사를 관리하는 데 필요한 모든 것을 수록하고 있는 엔터프라이즈 관리 도구입니다. CA Access Control 엔터프라이즈 관리 인터페이스에는 호스트를 구성하고, 정책을 만들어 할당하고, 사용자/그룹/관리 작업을 관리하고, 회사 전체에서 권한 있는 계정에 대한 액세스를 구성/관리하기 위한 도구가 포함되어 있습니다. 또한 엔터프라이즈 보고 및 감사 기능도 포함되어 있습니다.

중앙 정책 관리

회사의 호스트 또는 호스트 그룹에 일관된 정책을 만들어 할당하려면 CA Access Control 엔터프라이즈 관리의 중앙 정책 관리 기능을 사용하십시오. CA Access Control 엔터프라이즈 관리 인터페이스에서는 마법사를 사용하여 회사 전체에 적용되는 정책을 할당하고 모든 호스트에서 배포 프로세스 상태를 확인할 수 있습니다.

또한 CA Access Control 엔터프라이즈 관리 중앙 정책 관리 기능을 사용하여 정책 배포 프로세스의 문제를 해결하고, 기존 정책을 할당 취소하거나 업그레이드/다운그레이드할 수 있습니다.

엔터프라이즈 뷰

CA Access Control 엔터프라이즈 관리를 사용하여 중앙 위치에서 CA Access Control, PUPM, UNAB 호스트에 대한 정보를 보고 관리할 수 있습니다. CA Access Control 엔터프라이즈 관리 월드 뷰는 각 호스트 유형, 마지막 업데이트된 날짜, 각 호스트에 구성된 장치 유형에 대한 세부 정보를 표시하고, 호스트 설정을 수정하고 원격으로 관리할 수 있게 해 줍니다.

권한 있는 사용자 암호 관리

권한 있는 사용자 암호 관리(PUPM)는 회사에서 가장 강력한 계정과 관련된 모든 활동을 추적하고, 관리하고, 보안을 유지하기 위한 프로세스입니다.

CA Access Control 엔터프라이즈 관리를 사용하면 중앙 위치에서 관리되는 장치에 있는 권한 있는 계정의 액세스 권한을 역할에 기반하여 관리할 수 있습니다. CA Access Control 엔터프라이즈 관리는 권한 있는 계정 및 응용 프로그램 ID 암호를 안전하게 저장하고 정책에 기반하여 권한 있는 계정 및 암호에 대한 액세스를 제어합니다.

또한 CA Access Control 엔터프라이즈 관리를 사용하여 권한 있는 계정 및 응용 프로그램 암호를 관리하고 구성 파일 및 스크립트에서 암호를 제거할 수 있습니다.

UNAB 관리

UNIX 인증 브로커(UNAB)는 Active Directory 데이터 저장소를 사용하여 UNIX 컴퓨터에 로그인할 수 있게 해 줍니다. 즉, 모든 사용자에 대해 단일 리포지토리를 사용할 수 있으므로 사용자들이 동일한 사용자 이름과 암호를 사용하여 모든 플랫폼에 로그인할 수 있게 됩니다.

UNIX 계정을 Active Directory 와 통합하면 엄격한 인증 및 암호 정책을 시행하고, 기본 UNIX 사용자 및 그룹 속성을 Active Directory 로 전송할 수 있습니다. 이렇게 하면 Windows 사용자와 그룹을 관리할 때처럼 단일 지점에서 UNIX 사용자 및 그룹을 관리할 수 있게 됩니다.

일련의 로그인 규칙을 포함하는 로그인 정책을 만들어 할당하는 방법으로 UNIX 호스트에 대한 액세스를 제어하려면 CA Access Control 엔터프라이즈 관리 중앙 정책 관리 기능을 사용하십시오.

엔터프라이즈 보고서

CA Access Control 엔터프라이즈 관리 보고 옵션을 사용하면 한 위치에서 각 끝점(사용자, 그룹, 리소스)의 보안 상태를 볼 수 있습니다. 예약을 통해 또는 요청 시에 각 끝점에서 데이터를 수집할 수 있습니다. 어떤 사용자가 어떤 리소스에 액세스할 수 있는 권한이 있는지 확인하기 위해 각 끝점에 일일이 연결할 필요가 없습니다.

CA Access Control 보고 서비스는 한 번 설치되면 각 끝점에서 데이터를 수집하여 중앙 서버에 보고하기 위해 독립적으로 작동하며 사용자가 수동 작업을 할 필요 없이 끝점 상태를 계속 보고합니다. 즉 수집 서버가 가동되고 있는지 또는 중지되었는지에 관계없이 각 끝점에서 해당 상태를 보고합니다.

CA Access Control 엔터프라이즈 관리에는 즉시 사용할 수 있도록 각 끝점에 대한 일련의 정보를 표시하는 미리 정의된 보고서가 포함되어 있습니다. 또한 기존 보고서를 사용자 지정하여 원하는 정보를 수록하는 새 보고서를 만들 수 있습니다.

제 2 장: CA Access Control 엔터프라이즈 관리 관리

이 장은 아래의 주제를 포함하고 있습니다.

관리 범위 지정

CA Access Control 엔터프라이즈 관리에서는 관리 및 권한 있는 액세스 역할을 할당하여 사용자 및 관리자에게 사용 권한을 할당합니다. 역할은 CA Access Control 엔터프라이즈 관리의 응용 프로그램 기능에 해당하는 작업을 포함하고 있습니다.

역할은 사용함으로써 사용 권한을 쉽게 관리할 수 있습니다. 사용자에게 수행할 각 작업을 할당하지 않고 대신 사용자에게 역할을 할당할 수 있습니다. 사용자는 자신의 할당된 역할에 있는 모든 작업을 수행할 수 있습니다. 그런 다음 작업을 추가하여 역할을 수정할 수 있습니다. 그러면 이 역할이 있는 모든 사용자는 이제 새 작업을 수행할 수 있게 됩니다. 역할에서 하나의 작업을 제거하면 해당 사용자는 더 이상 이 작업을 수행할 수 없습니다.

사용자가 CA Access Control 엔터프라이즈 관리에 로그인하면 자신의 역할에 해당하는 탭을 보게 됩니다. 사용자는 자신의 역할에 할당된 탭 및 작업만 볼 수 있습니다.

하나의 사용자가 모든 작업을 수행하는 것을 방지하려면 다른 여러 사용자에게 다른 역할을 할당할 수 있습니다. 이렇게 하면 회사의 권한 분리 원칙을 충족시키는 데 도움이 됩니다. 하지만 한 사용자에게 여러 역할을 할당할 수 있습니다.

CA Access Control 엔터프라이즈 관리의 관리 역할

CA Access Control 엔터프라이즈 관리의 미리 정의된 관리 역할은 필요에 따라 회사의 관리자에게 할당할 수 있는 기본 관리 역할 세트를 제공합니다. CA Access Control 엔터프라이즈 관리에는 다음과 같은 즉시 사용 가능한 관리 역할이 기본적으로 포함되어 있습니다.

- **CA Access Control 호스트 관리자** - 호스트 및 로컬 호스트 그룹을 정의합니다.

  이 관리 역할이 있는 사용자는 호스트 및 호스트 그룹을 만들고, 호스트를 호스트 그룹에 할당하고, 이들을 수정할 수 있습니다. 이 역할의 사용자는 정책 또는 배포 정책을 정의할 수는 없지만 이러한 정책을 보고 월드 뷰에 액세스할 수 있습니다.

- **CA Access Control 정책 배포자** - 환경 전체에서 정책을 배포합니다.

  이 관리 역할이 있는 사용자는 정책을 호스트 및 호스트 그룹에 할당하고, 정책을 업그레이드/다운그레이드하고, 구성을 다시 설정하고, 배포 감사에 액세스할 수 있습니다. 이 역할의 사용자는 정책 및 호스트를 볼 수 있지만 정의할 수는 없으며 월드 뷰에 액세스할 수 있습니다.

- **CA Access Control 정책 관리자** - 정책을 만듭니다.

  이 관리 역할이 있는 사용자는 정책을 만들고, 수정하고, 보고, 삭제할 수 있습니다. 이 역할의 사용자는 호스트 또는 호스트 그룹에 정책을 배포할 수는 없지만 이들을 보고 월드 뷰에 액세스할 수 있습니다.

- **CA Access Control 사용자 관리자** - CA Access Control 엔터프라이즈 관리에서 사용자를 관리합니다. 즉, 사용자 및 그룹을 만들고 관리하며 CA Access Control 엔터프라이즈 관리 역할을 사용자에게 할당합니다.

  참고: CA Access Control 사용자 관리자는 새 관리 역할을 만들 수 없습니다. 시스템 관리자만 새 관리 역할을 만들 수 있습니다.

- **시스템 관리자** - CA Access Control 엔터프라이즈 관리를 관리합니다.

  이 관리 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리에 있는 모든 작업을 수행하고, 만들고, 관리할 수 있습니다.

  회사에서 실제 관리 역할을 정의하는 구현 단계와 비상 상황에 이 역할을 사용하십시오. 이 역할을 최소한의 사용자에게 할당하고(사용자 한 명이 적합함) 이 사용자의 동작을 자세히 모니터링하는 것이 좋습니다.

- **보고** - 영어 보고서를 관리합니다. 이 역할이 있는 사용자는 보고서를 예약하고 볼 수 있습니다.

- **UNAB 관리자** - UNAB 를 관리합니다. 이 역할이 있는 사용자는 UNAB 호스트 및 호스트 그룹을 구성하고, 로그인 권한 부여 정책을 관리하고, 마이그레이션 충돌을 해결할 수 있습니다.

  참고: 시스템 관리자 역할이 할당된 사용자에게는 UNAB 관리자 역할도 함께 할당됩니다.

- **보고 JP** - 일본어 보고서를 관리합니다. 이 역할이 있는 사용자는 보고서를 예약하고 볼 수 있습니다.

- **보고 KO** - 한국어 보고서를 관리합니다. 이 역할이 있는 사용자는 보고서를 예약하고 볼 수 있습니다.

- **CA Enterprise Log Manager 사용자** - CA Enterprise Log Manager 보고서를 볼 수 있습니다. 이 역할이 있는 사용자는 CA Enterprise Log Manager 보고서를 볼 수 있습니다.

- **CA Enterprise Log Manager 관리자** - CA Enterprise Log Manager 보고서를 관리합니다. 이 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리에서 CA Enterprise Log Manager 보고서를 관리하고 CA Enterprise Log Manager 서버에 대한 연결을 관리할 수 있습니다.

- **위임 관리자** - 작업 항목을 위임합니다. 이 역할이 있는 사용자는 작업 항목을 사용자에게 위임할 수 있습니다.

- **자체 관리자** - 자신의 사용자 계정을 관리합니다. 이 역할이 있는 사용자는 자신의 계정에서 계정 암호 변경, 자신의 사용자 프로필 수정, 자신의 할당된 역할/제출된 작업/승인 대기 중인 항목 보기와 같은 관리 작업을 수행할 수 있습니다.

  참고: 기본적으로 시스템 모든 사용자에게는 자체 관리자 역할이 할당됩니다.

관리자 역할 만들기

CA Access Control 엔터프라이즈 관리에 있는 미리 정의된 관리 역할이 조직 요구 사항에 적합하지 않은 경우 새 역할을 만들 수 있습니다.

관리자 역할을 만들려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "사용자 및 그룹"을 클릭합니다.
   b. "역할" 하위 탭을 클릭합니다.
   c. 작업 메뉴에서 왼쪽에 있는 "관리 역할" 트리를 확장합니다.

      사용 가능한 작업 목록에 "관리 역할 만들기" 작업이 나타납니다.
2. "관리 역할 만들기"를 클릭합니다.

   "관리 역할 만들기: 관리 역할 선택" 페이지가 나타납니다.
3. (선택 사항) 다음과 같이 새 관리 역할을 만들 때 복사하여 사용할 기존 관리 역할을 선택합니다.
   a. "역할 복사본 만들기"를 선택합니다.
   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 관리 역할의 목록이 나타납니다.
   c. 새 관리 역할을 만들 때 기초로 사용할 개체를 선택합니다.
4. "확인"을 클릭합니다.

   "관리 역할 만들기" 작업 페이지가 나타납니다. 기존 개체에서 관리 역할을 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.
5. 대화 상자의 "프로필" 탭에서 다음 필드를 완성합니다.

   이름

   역할의 이름을 정의합니다.

   설명

   역할에 대한 설명합니다.

   사용

   역할이 사용자 및 그룹에 할당될 수 있는지 여부를 지정합니다.

6. 다음과 같이 역할에 작업을 추가합니다.
   a. "작업" 탭을 클릭합니다.
   b. (선택 사항) "필터" 작업 드롭다운 목록에서 작업 범주를 선택합니다.

      이 범주의 작업이 로드됩니다.

      참고: 작업 범주는 이 범주의 작업이 CA Access Control 엔터프라이즈 관리에 나타나는 탭과 일치합니다.
   c. "작업 추가" 드롭다운 목록에서 작업을 선택합니다.

      작업이 역할에 추가됩니다.
   d. b 에서 c 단계를 반복하여 역할에 작업을 더 추가합니다.
7. 구성원 및 범위 규칙을 추가합니다(페이지 26).
8. "제출"을 클릭합니다.

   이렇게 하면 역할이 만들어집니다.

권한 있는 액세스 역할

CA Access Control 엔터프라이즈 관리의 권한 있는 액세스 역할은 필요에 따라 회사의 관리자 및 사용자에게 할당할 수 있는 기본 규칙 세트를 제공합니다. CA Access Control 엔터프라이즈 관리에는 다음과 같은 즉시 사용 가능한 권한 있는 액세스 역할이 기본적으로 포함되어 있습니다.

- **Break Glass** - 이 역할이 있는 사용자는 Break Glass 권한 있는 계정 암호 체크 아웃을 시작할 수 있습니다. Break Glass 체크 아웃을 사용하면 사용자에게 액세스 권한이 없는 끝점에 즉시 액세스할 수 있습니다. 이 역할은 기본적으로 CA Access Control 엔터프라이즈 관리의 모든 사용자에게 할당됩니다.
- **끝점 권한 있는 액세스 규칙** - 이 역할이 있는 사용자는 지정된 끝점 유형에서 권한 있는 액세스 작업을 수행할 수 있습니다. 새 끝점 유형을 처음 정의할 때 CA Access Control 은 해당 끝점 권한 있는 액세스 역할을 만듭니다. 예를 들어, CA Access Control 엔터프라이즈 관리에 처음 Windows 끝점을 만들면 CA Access Control 이 Windows Agentless 연결 끝점 권한 있는 액세스 역할을 만듭니다.
- **권한 있는 계정 요청** - 이 역할이 있는 사용자는 권한 있는 계정 암호에 대한 요청을 제출 또는 삭제할 수 있습니다. 이 역할은 기본적으로 CA Access Control 엔터프라이즈 관리의 모든 사용자에게 할당됩니다.
- **PUPM 승인자** - 이 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리 사용자가 제출한 권한 있는 액세스 요청에 응답할 수 있습니다. 이 역할은 기본적으로 CA Access Control 엔터프라이즈 관리의 모든 사용자에게 할당됩니다.

- **PUPM 감사 관리자** - 이 역할이 있는 사용자는 권한 있는 계정 활동을 감사하고 CA Enterprise Log Manager 감사 수집 매개 변수를 관리할 수 있습니다.
- **PUPM 정책 관리자** - 이 역할이 있는 사용자는 역할 구성원과 구성원 정책을 관리할 수 있고, 역할 소유자를 할당할 수 있고, 역할을 생성 및 삭제할 수 있습니다.
- **PUPM 대상 시스템 관리자** - 이 역할이 있는 사용자는 암호 정책 및 권한 있는 계정을 관리할 수 있고, 끝점에서 권한 있는 계정을 검색하기 위해 권한 있는 계정 검색 마법사를 실행할 수 있습니다.
- **PUPM 사용자** - 이 역할이 있는 사용자는 사용이 허가된 권한 있는 계정 암호를 체크 인 및 체크 아웃할 수 있습니다. 이 역할은 기본적으로 CA Access Control 엔터프라이즈 관리의 모든 사용자에게 할당됩니다.
- **PUPM 사용자 관리자** - 이 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리 사용자, 그룹, 암호 정책을 관리하고 사용자의 작업 항목을 관리할 수 있습니다.

사용자에게 권한 있는 액세스 역할을 할당할 때는 다음 사항에 주의해야 합니다.

- 권한 있는 계정 요청에 응답하려면 사용자에게 PUPM 승인자 역할이 있어야 하며 요청하는 사용자의 관리자여야 합니다.
- 사용자에게 Break Glass, 권한 있는 계정 요청 또는 PUPM 사용자 역할이 있지만 끝점 권한 있는 액세스 역할이 없는 경우 이 사용자는 어떠한 끝점에도 액세스할 수 없습니다. 결과적으로 이 사용자는 어떠한 작업도 수행 수 없게 됩니다.
- 사용자에게 끝점 권한 있는 액세스 역할이 있지만 다른 역할이 없는 경우 이 사용자는 어떠한 작업도 수행할 수 없습니다.

권한 있는 액세스 역할 만들기

권한 있는 액세스 역할은 역할 구성원, 관리자, 소유자가 PUPM 을 사용할 때 수행할 수 있는 작업(예: 권한 있는 계정 체크 인 및 체크 아웃)를 정의합니다. CA Access Control 엔터프라이즈 관리에 있는 미리 정의된 권한 있는 액세스 역할이 조직 요구 사항에 적합하지 않은 경우 새 역할을 만들 수 있습니다.

권한 있는 액세스 역할을 만들려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "사용자 및 그룹"을 클릭합니다.
   b. "역할" 하위 탭을 클릭합니다.
   c. 작업 메뉴에서 왼쪽에 있는 "권한 있는 액세스 역할" 트리를 확장합니다.

      사용 가능한 작업 목록에 "권한 있는 액세스 역할 만들기" 작업이 나타납니다.
2. "권한 있는 액세스 역할 만들기"를 클릭합니다.

   "역할 만들기: 권한 있는 액세스 역할 선택" 페이지가 나타납니다.
3. (선택 사항) 다음과 같이 새 역할을 만들 때 복사하여 사용할 기존 권한 있는 액세스 역할을 선택합니다.
   a. "역할 복사본 만들기"를 선택합니다.
   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 권한 있는 액세스 역할의 목록이 나타납니다.
   c. 새로운 권한 있는 액세스 역할을 만들 때 기초로 사용할 개체를 선택합니다.
4. "확인"을 클릭합니다.

   "관리 역할 만들기" 작업 페이지가 나타납니다. 기존 개체에서 관리 역할을 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.
5. 대화 상자의 "프로필" 탭에서 다음 필드를 완성합니다.

   이름

   역할의 이름을 정의합니다.

   설명

   역할에 대한 설명합니다.

   사용

   역할이 사용자 및 그룹에 할당될 수 있는지 여부를 지정합니다.

6. 다음과 같이 역할에 작업을 추가합니다.
   a. "작업" 탭을 클릭합니다.
   b. (선택 사항) "필터" 작업 드롭다운 목록에서 작업 범주를 선택합니다.

      이 범주의 작업이 로드됩니다.

      참고: 작업 범주는 이 범주의 작업이 CA Access Control 엔터프라이즈 관리에 나타나는 탭과 일치합니다.
   c. "작업 추가" 드롭다운 목록에서 작업을 선택합니다.

      작업이 역할에 추가됩니다.
   d. b 에서 c 단계를 반복하여 역할에 작업을 더 추가합니다.
7. 구성원 및 범위 규칙을 추가합니다(페이지 26).
8. "제출"을 클릭합니다.

   이렇게 하면 역할이 만들어집니다.

사용자에게 역할을 할당하는 방법

다음 방법을 사용하여 사용자에게 역할을 할당할 수 있습니다:

- "역할 구성원/관리자 수정" 작업을 사용하여 역할에서 여러 사용자를 추가 또는 제거할 수 있습니다.
- "사용자 수정" 작업의 "권한 있는 액세스 역할" 탭 또는 "관리 역할" 탭을 사용하여 한 사용자에 대해 역할을 추가 또는 제거할 수 있습니다.
- "권한 있는 액세스 역할 수정" 탭 또는 "관리 역할 수정" 작업에 있는 "구성원" 탭을 사용하여 역할에 대한 구성원 정책을 수정합니다.

사용자를 관리 역할에 추가하는 방법

관리 역할을 만든 다음에는 이 역할에 구성원과 관리자를 추가할 수 있습니다. 역할의 구성원인 사용자는 해당 역할에 부여된 권한을 할당합니다. 다음 단계는 역할에 구성원을 추가하기 위한 사전 요구 사항입니다.

1. 이 규칙의 구성원을 정의하기 위해 관리 역할 구성원 정책 정의를 수정합니다.

   다른 역할의 구성원인 사용자를 수정하는 역할에 추가하도록 허용하는 역할 구성원 정책을 수정합니다.

   예: 여기서 로그온 이름 = "Administrator" 또는 관리 역할 = "SystemManager"

2. 관리자(administrator)가 이 역할에서 구성원을 추가 또는 제거할 수 있는지 확인합니다.
3. 이 역할에서 사용자가 추가 또는 제거될 때 발생하는 동작을 정의합니다.

   예: 관리 역할에 SystemManager 추가, 관리 역할에서 SystemManager 제거
4. 사용자를 관리 규칙에 있는 이 역할에 관리자로 추가하고 사용자에게 관리자 권한을 할당하기 위해 관리 정책을 수정합니다.

   역할 관리자로 할당한 사용자가 이 역할에 구성원을 추가하도록 권한 부여됩니다.

   이제 이 역할에 구성원을 추가할 수 있습니다.

구성원 및 범위 규칙 추가

역할의 프로필과 작업을 정의한 다음에는 구성원, 관리자, 소유자를 추가합니다.

구성원 및 범위 규칙을 추가하려면

1. "구성원" 탭을 클릭한 후 다음 중 하나를 수행합니다.
   a. "추가"를 클릭합니다.
   b. 구성원 정책(페이지 28)에 대한 구성원 규칙과 범위 규칙을 지정한 다음 "확인"을 클릭합니다.
   c. (선택 사항) 관리자가 이 역할의 구성원을 추가 및 제거할 수 있도록 선택하고 작업 추가 및 작업 제거(페이지 28)를 지정합니다.

   역할의 구성원 정책이 만들어집니다.
2. "관리자" 탭을 클릭한 후 다음 중 하나를 수행합니다.
   a. "추가"를 클릭합니다.
   b. 관리 규칙과 범위 규칙을 지정하고 관리 정책(페이지 29)에 대한 관리자 권한을 지정한 다음 "확인"을 클릭합니다.
   c. (선택 사항) 관리자가 이 규칙의 관리자를 추가 및 제거할 수 있도록 선택하고 작업 추가 및 작업 제거(페이지 28)를 지정합니다.

   역할의 관리 정책이 만들어집니다.
3. "소유자" 탭을 클릭한 다음 "추가"를 클릭하고 소유자 역할(페이지 29)을 지정한 다음 "확인"을 클릭합니다.

   정책의 소유자 규칙이 만들어집니다.

구성원 정책

구성원 정책은 역할에서 작업을 수행할 수 있는 사용자를 정의합니다. 구성원 정책에는 다음이 포함되어 있습니다.

- **구성원 규칙** - 역할을 수행할 수 있는 사용자를 정의합니다.
- **범위 규칙** - 사용자가 관리할 수 있는 개체를 정의합니다.

예를 들어, 관리 역할, 연결, 권한 있는 계정, 정책은 모두 개체입니다. 범위 규칙에 많은 다른 개체를 지정할 수 있습니다. 각 구성원 정책에는 둘 이상의 구성원 규칙이 있을 수 있으며 각 구성원 규칙에는 둘 이상의 범위 규칙이 있을 수 있습니다.

예: 뉴욕 CA Access Control 호스트 관리자의 구성원 정책

Don Hailey 는 Forward, Inc 의 IT 관리자로서 시스템 관리자 관리자 역할을 가지고 있습니다. Don 은 뉴욕 사무소에서 CA Access Control 호스트 관리자 관리 역할이 있는 직원이 Forward, Inc 뉴욕 사무소에 있는 호스트 및 호스트 그룹만 관리하는 관리 역할을 만들려고 합니다. 모든 뉴욕 직원들은 NY 직원 그룹의 구성원이며 뉴욕의 모든 호스트 및 호스트 그룹의 이름은 NY 라는 문자로 시작합니다.

Don 이 다음과 같이 구성원 정책을 작성합니다. 구성원 정책에는 두 개의 구성원 규칙이 포함되어 있습니다. 첫 번째 구성원 규칙에는 범위 규칙이 없습니다. 두 번째 구성원 규칙에 다음과 같은 두 개의 범위 규칙이 포함되어 있습니다.

- 구성원 규칙 1 - 관리자 역할에 "AC 호스트 관리자"가 포함됩니다.
- 구성원 규칙 2 - "NY 직원" 그룹의 구성원인 사용자. 범위 규칙 - 이름이 "NY"로 시작하는 호스트 및 이름이 "NY"로 시작하는 호스트 그룹

추가 및 제거 작업

관리 역할의 관리자가 사용자에게 특정 역할을 할당하거나 사용자에 할당된 역할을 할당 취소할 수 있도록 하려면 해당 관리 역할에 대해 "추가" 및 "제거" 작업을 지정해야 합니다.

추가 및 제거 작업은 다음을 포함합니다.

- **추가 작업** - 사용자가 역할 구성원 규칙 중 하나의 조건을 충족하도록 합니다.
- **제거 작업** - 사용자가 역할 구성원 규칙 중 하나의 조건을 더 이상 충족하지 않도록 합니다.

관리자 정책

관리자 정책은 관리 역할의 관리자인 사용자를 지정합니다. 관리 역할 관리자는 관리 역할의 구성원 정책을 관리하고, 관리 역할에 사용자 및 그룹을 추가하거나 관리 역할에서 사용자 및 그룹을 제거합니다.

관리자 정책은 다음을 포함합니다.

- **관리 규칙** - 규칙의 관리자인 사용자를 정의합니다.
- **범위 규칙** - 관리자가 관리할 수 있는 사용자를 정의합니다.
- **관리자의 권한** - 관리자가 관리 역할의 구성원 및 관리자를 관리할 수 있는지 여부를 지정합니다.

역할 소유자

역할 소유자는 관리 역할에 작업을 추가하거나 관리 역할에서 작업을 제거합니다. 소유자 규칙은 단 하나만 정의할 수 있지만 소유자 규칙 내에서 여러 그룹의 구성원을 지정할 수 있습니다.

관리 작업 만들기

CA Access Control 엔터프라이즈 관리에 있는 미리 정의된 관리 작업이 조직 요구 사항에 적합하지 않은 경우 새 관리 작업을 만들 수 있습니다.

관리 작업을 만들려면

1. "사용자 및 그룹" 탭을 선택하고 "작업" 링크를 선택한 다음 "관리 작업 만들기"를 클릭합니다.

   "관리 작업 만들기: 관리 작업 선택" 페이지가 나타납니다.

2. 새 관리 작업을 만들도록 선택한 다음 "확인"을 클릭합니다.

   "관리 작업 만들기" 페이지의 "프로필" 탭이 나타납니다.

   참고: 기존 관리 작업의 복사본을 만들려면 관리 작업의 복사본을 만들도록 선택하고, 복사할 관리 작업을 검색하고, 관리 작업을 선택한 다음 "확인"을 클릭합니다.

3. 작업 이름과 설명을 입력합니다. 필드에 커서를 가져가면 태그 필드에 이름이 표시됩니다.
4. 메뉴의 작업 목록에서 작업의 위치를 선택합니다.
5. 이 작업이 속한 범주를 선택합니다.
6. (선택 사항) 최대 3 개까지 작업의 순서 및 범주 이름을 선택합니다.
7. 이 작업이 속한 주 개체를 선택합니다. 주 개체는 이 작업에 대한 가장 높은 범주입니다.

8. 작업과 연계할 동작을 선택합니다.
9. 사용자와 계정을 작업과 동기화할지 여부를 선택합니다.
10. 다음 옵션 중 하나를 선택합니다.

메뉴에서 숨기기

작업을 표시하지 않습니다.

공용 작업

모든 사용자가 작업을 사용할 수 있도록 선택합니다.

감사 사용

이 작업에 대해 감사 이벤트 로깅을 사용하도록 선택합니다.

작업흐름 사용

작업흐름을 사용하도록 설정합니다.

웹 서비스 사용

웹 서비스를 사용하여 이 작업에 액세스할 수 있도록 선택합니다.

작업흐름 프로세스

작업과 연계할 작업흐름 프로세스를 선택합니다.

11. 작업 우선 순위를 선택합니다.
12. "제출"을 선택합니다.

CA Access Control 엔터프라이즈 관리가 관리 작업을 만듭니다.

추가 정보:

검색 화면 추가(페이지 31)
탭 추가(페이지 31)
필드, 이벤트, 역할 사용 구성(페이지 31)

검색 화면 추가

이 작업과 연계할 검색 화면을 선택합니다. 이 탭에서는 이 작업에서 기존 검색 화면을 사용하거나, 정보를 표시하고 이 작업에 고유한 검색 옵션을 제공하는 새 검색 화면을 만들 수 있습니다.

검색 화면을 추가하려면

1. 찾아보기 단추를 클릭하여 기존 검색 화면을 찾거나 새 검색 화면을 만듭니다.

   참고: 기존 검색 화면의 복사본을 만들려면 다른 작업에서 범위를 복사하고, 복사할 관리 작업을 검색하고, 관리 작업을 선택한 다음 "확인"을 클릭합니다.

2. "새로 만들기"를 선택하여 새 검색 화면을 만듭니다.
3. 만들 검색 화면의 유형을 선택합니다.
4. 필요한 정보를 입력한 다음 "확인"을 클릭합니다.

   작업에 새 검색 화면이 추가됩니다.

탭 추가

이 작업에 사용할 탭 컨트롤러를 선택하고 작업에 표시될 탭을 선택하려면 탭 화면을 사용하십시오.

탭을 추가하려면

1. 이 작업에 사용할 탭 컨트롤러를 선택합니다.

   참고: 기존 탭 정의의 복사본을 만들려면 다른 작업에서 탭을 복사하도록 선택하고, 복사할 관리 작업을 검색하고, 관리 작업을 선택한 다음 "확인"을 클릭합니다.

2. 메뉴에서 이 작업에 표시될 탭을 선택합니다.
3. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 해당 탭을 새 작업에 추가합니다.

필드, 이벤트, 역할 사용 구성

필드, 이벤트, 역할 사용 탭은 이 작업이 액세스하는 필드, 작업에 연결된 이벤트, 이 작업을 볼 수 있는 사용자 역할과 관련된 정보를 표시합니다. 이 필드에 표시된 정보는 변경할 수 없습니다.

설정을 변경하여 이 탭에 표시되는 정보를 변경할 수 있습니다. 예를 들어, 이 작업이 표시되는 관리 역할을 변경하려면 이 작업을 포함 또는 제외하도록 관리 역할 설정을 수정하십시오.

사용자, 그룹, 관리 역할

사용자를 만들 때 하나 이상의 관리 역할 또는 권한 있는 액세스 역할을 할당합니다. 관리 역할은 CA Access Control 엔터프라이즈 관리의 응용 프로그램 기능에 해당하는 작업을 포함하고 있습니다. 사용자에게 관리 역할을 할당하면 이 사용자는 관리 역할에 포함된 작업을 수행할 수 있습니다. 작업은 정책을 만들고, 정책을 배포하고, 호스트 그룹을 만들고, 다른 사용자를 관리하는 것과 같은 CA Access Control 기능을 수행할 수 있게 해줍니다.

권한 있는 액세스 역할은 관리되는 끝점에서 권한 있는 계정 관리에 해당하는 작업을 정의합니다. 권한 있는 액세스 역할을 사용자에게 할당하면 이 사용자는 권한 있는 계정 암호 검사와 같은 권한 있는 계정 관리 작업을 수행할 수 있습니다.

간편한 관리를 위해 사용자의 그룹을 만든 다음 이 그룹에 관리 역할을 할당할 수 있습니다. 이렇게 하면 그룹 내의 각 사용자가 해당 관리 역할에 포함된 모든 작업을 수행할 수 있게 됩니다.

추가 정보:

사용자 만들기(페이지 33)
그룹 유형(페이지 36)

Active Directory 제한

사용자 저장소로 Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리에서 사용자 및 그룹을 만들거나 삭제할 수 없습니다. 인터페이스에서 다음 작업을 볼 수 없으며 이러한 작업을 관리 역할 또는 권한 있는 액세스 역할에 할당할 수 없습니다.

- 사용자 만들기
- 사용자 삭제
- 그룹 작성
- 그룹 삭제

이러한 제한은 CA Access Control 엔터프라이즈 관리를 설치하고 사용자 저장소로 Active Directory 를 지정할 때 CA Access Control 이 Active Directory 에 프록시 사용자를 만들기 때문에 발생합니다. 이 프록시 사용자는 Active Directory 에서 사용자 및 그룹을 만들고 삭제하기 위해 필요한 권한이 없습니다.

사용자 만들기

사용자는 CA Access Control 엔터프라이즈 관리에서 작업을 수행합니다. CA Access Control 엔터프라이즈 관리를 설치할 때 시스템 관리자 역할이 있는 사용자를 만듭니다. CA Access Control 엔터프라이즈 관리를 시작하여 권한 분리를 시행할 때 추가 사용자를 만드십시오.

참고: 사용자 저장소로 Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리에 사용자를 만들 수 없습니다.

사용자를 만들려면

1. CA Access Control 엔터프라이즈 관리에서 "사용자 및 그룹"을 클릭합니다.

   사용 가능한 작업 목록에 "사용자 만들기" 작업이 나타납니다.

2. "사용자 만들기"를 클릭합니다.

   "사용자 만들기: 사용자 선택" 창이 나타납니다.

3. (선택 사항) 다음과 같이 새 사용자를 만들 때 복사하여 사용할 기존 사용자를 선택합니다.

   a. 사용자의 복사본 만들기를 선택합니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 사용자의 목록이 표시됩니다.

   c. 새 사용자를 만들 때 기초로 사용할 개체를 선택합니다.

4. "확인"을 클릭합니다.

   "사용자 만들기" 작업 페이지가 나타납니다. 기존 개체에서 사용자를 만든 경우 기존 개체의 값이 대화 상자 필드에 미리 입력됩니다.

5. "프로필" 탭에서 이 필드를 완성합니다. 다음 필드는 자동으로 채워지지 않습니다.

   사용자 ID

   CA Access Control 엔터프라이즈 관리에서 사용자를 식별하는 문자열을 정의합니다. 이 문자열은 로그인하는 데 사용하는 사용자의 이름입니다.

   암호를 반드시 변경

   사용자가 처음 로그인할 때 암호를 반드시 변경하도록 지정합니다.

   사용

   사용자가 CA Access Control 엔터프라이즈 관리에 로그인할 수 있는지 여부를 지정합니다.

6. (선택 사항) "관리 역할"을 클릭하여 다음과 같이 사용자에게 관리 역할을 할당합니다.
   a. 관리 역할 추가를 클릭합니다.

      "관리 역할 선택" 섹션이 나타납니다.

   b. 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 역할의 목록이 표시됩니다.

   c. 사용자에게 할당할 관리 역할을 선택한 다음 "선택"을 클릭합니다.

   사용자에게 관리 역할이 할당됩니다.
7. (선택 사항) "권한 있는 액세스 역할" 탭을 클릭하여 다음과 같이 사용자에게 권한 있는 액세스 역할을 할당합니다.
   a. 권한 있는 액세스 역할 추가를 클릭합니다.

      "권한 있는 액세스 역할 선택" 섹션이 나타납니다.

   b. 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 역할의 목록이 표시됩니다.

   c. 사용자에게 할당할 권한 있는 액세스 역할을 선택한 다음 "선택"을 클릭합니다.

   사용자에게 권한 있는 액세스 역할이 할당됩니다.
8. (선택 사항) "그룹" 탭을 클릭하여 다음과 같이 사용자를 그룹에 추가합니다.
   a. 그룹 추가를 클릭합니다.

      "그룹 선택" 섹션이 나타납니다.

   b. 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 그룹의 목록이 표시됩니다.

   c. 사용자에게 할당할 그룹을 선택한 다음 "선택"을 클릭합니다.

   그룹에 사용자가 추가됩니다.
9. "제출"을 클릭합니다.

   사용자가 만들어집니다.

사용자 암호 다시 설정

여러 번 로그인에 실패하여 계정이 잠기거나 암호를 잊어버린 경우 사용자 암호를 다시 설정합니다.

사용자 암호를 다시 설정하려면

1. CA Access Control 엔터프라이즈 관리에서 "사용자 및 그룹"을 클릭합니다.

   사용 가능한 작업의 목록에 "사용자 암호 다시 설정"이 표시됩니다.

2. "사용자 암호 다시 설정"을 클릭합니다.

   "사용자 암호 다시 설정" 검색 페이지가 열립니다.

3. 검색 쿼리를 입력한 다음 "검색"을 클릭합니다.

   검색 조건에 따라 쿼리 결과가 표시됩니다.

4. 사용자 계정을 선택하고 "선택"을 클릭합니다.

   암호 다시 설정 창이 열립니다.

5. "암호 확인" 필드에 계정 암호를 입력합니다.

6. (선택 사항) "암호를 반드시 변경" 옵션을 선택합니다.

7. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 사용자 암호를 다시 설정합니다.

사용자 활성화 또는 비활성화

사용자가 계정 자격 증명을 사용하여 CA Access Control 엔터프라이즈 관리에 로그인할 수 있도록 하려면 사용자를 활성화합니다. 사용자가 CA Access Control 엔터프라이즈 관리에 액세스할 수 없도록 하고 시스템에 사용자 프로필을 유지하려면 사용자 계정을 비활성화합니다.

사용자를 활성화 또는 비활성화하려면

1. CA Access Control 엔터프라이즈 관리에서 "사용자 및 그룹"을 클릭합니다.

   사용 가능한 작업 목록에 "사용자 활성화/비활성화" 작업이 나타납니다.

2. "사용자 활성화/비활성화"를 클릭합니다.

   "사용자 활성화/비활성화" 페이지가 나타납니다.

3. 검색 쿼리를 정의하고 "검색"을 클릭합니다.

   검색 쿼리에 일치하는 사용자의 목록이 표시됩니다.

4. 다음과 같이 활성화 및 비활성화할 사용자 계정을 지정합니다.
   - 계정을 비활성화할 사용자를 지웁니다.
   - 계정을 활성화할 사용자를 선택합니다.
5. 선택을 클릭합니다.

   지정한 변경 내용을 요약하는 화면이 표시됩니다.
6. "예"를 클릭하여 수정 내용을 승인합니다.

   CA Access Control 엔터프라이즈 관리는 작업을 제출하여 요청된 변경을 수행합니다.

그룹 유형

여러 유형의 그룹이나 이러한 유형의 조합을 만들 수 있습니다.

- **정적 그룹**

  대화형으로 추가된 일련의 사용자입니다.
- **동적 그룹**

  LDAP 쿼리를 충족하는 경우 그룹에 속하는 사용자입니다. 사용자 저장소로 LDAP 디렉터리가 요구됩니다.

  참고: 동적 그룹 쿼리 필드를 보려면 관련 프로필 화면을 편집하여 이 필드를 작업에 포함시켜야 합니다.
- **중첩 그룹**

  다른 그룹을 포함하는 그룹입니다. 사용자 저장소로 LDAP 디렉터리가 요구됩니다.

  참고: 사용자가 속한 정적, 동적, 중첩 그룹을 보려면 "사용자" 개체의 "그룹" 탭을 사용하십시오. 이 탭은 "사용자 보기" 및 "사용자 수정" 작업에 있습니다.

정적 또는 동적 그룹 만들기

사용자 모음을 정적 그룹으로 연결할 수 있습니다. 그룹의 구성원 자격 목록에서 사용자를 추가하거나 제거하여 그룹을 관리합니다. 그룹의 구성원 자격을 보려면 "그룹 보기" 또는 "그룹 수정" 작업에서 "구성원 자격" 탭을 사용하십시오.

CA Access Control 엔터프라이즈 관리를 사용하여 LDAP 필터 쿼리를 정의하는 방법으로 동적 그룹을 만들면 런타임에 그룹 구성원 자격을 파악할 수 있습니다.

참고: "구성원 자격" 탭에는 명시적으로 그룹에 추가된 구성원만 표시됩니다. 사용자 저장소로 Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리에 그룹을 만들 수 없습니다.

정적 또는 동적 그룹을 만들려면

1. 그룹 관리 권한이 있는 사용자로 CA Access Control 엔터프라이즈 관리에 로그인합니다.
2. "그룹", "그룹 만들기"를 차례로 선택합니다.

   그룹 만들기 검색 화면이 나타납니다.
3. 그룹을 만들도록 선택하고 "확인"을 클릭합니다.

   그룹 프로필 탭이 나타납니다.
4. 그룹 이름과 설명을 입력합니다.
5. "구성원 자격" 탭으로 이동합니다.

   참고: "그룹 수정" 작업이 있는 관리자만 그룹 동적 구성원 자격을 변경할 수 있습니다.
6. "사용자 추가"를 클릭합니다.

   사용자 선택 검색 창이 열립니다.
7. 검색 쿼리를 입력하고 "검색"을 클릭합니다.

   검색 조건에 따라 쿼리 결과가 반환됩니다.
8. 사용자를 선택하고 "선택"을 클릭합니다.

   "관리자" 탭으로 이동합니다.
9. "제출"을 클릭합니다.

   프로세스가 성공적으로 완료되었음을 알리는 메시지가 표시됩니다.

   참고: 사용자를 그룹 관리자로 할당하는 경우 관리자가 그룹 관리에 적합한 범위가 있는 역할을 가지고 있는지 확인하십시오.

LDAP 필터 쿼리 - 동적 그룹 쿼리 매개 변수 정의

CA Access Control 엔터프라이즈 관리를 사용하여 LDAP 필터 쿼리를 정의하는 방법으로 동적 그룹을 만들면 런타임에 그룹 구성원 자격을 파악할 수 있습니다.

이 필터 쿼리의 형식은 다음과 같습니다.

```
LDAP:///search_base_DN??search_scope?searchfilter
```

search_base_DN

LDAP 디렉터리에서 검색을 시작하는 지점을 정의합니다. 쿼리에 기본 DN 을 지정하지 않으면 그룹 조직이 기본 DN 이 됩니다.

search_scope

검색 범위를 지정하며 다음을 포함합니다.

- **sub** - 기본 DN 수준 및 그 아래의 항목을 반환합니다.
- **one** - URL 에 지정하는 기본 DN 보다 한 수준 아래의 항목을 반환합니다.
- **base** - 검색 옵션으로 base 를 무시하고 one 을 대신 사용합니다.

one 또는 base 를 사용하면 기본 DN 조직의 사용자만 반환됩니다.

sub 를 사용하면 기본 DN 조직 및 트리에서 모든 하위 조직의 사용자가 모두 반환됩니다.

searchfilter

검색 범위 내의 항목에 적용할 필터를 정의합니다. 검색 필터를 입력하는 경우 다음과 같은 표준 LDAP 쿼리 구문을 사용합니다.

```
([logical_operator]Comparison)
```

logical operator

논리 연산자를 정의합니다. 다음 중 하나일 수 있습니다.

- **|** - 논리적 OR
- **&** - 논리적 AND
- **!** - 논리적 NOT

Comparison

AttributeOperatorValue 를 정의합니다.

- Attribute - LDAP 특성의 이름을 정의합니다.
- Operator - 비교 연산자를 지정합니다. 다음 중 하나: **=** (같음), **<=** (작거나 같음), **>=** (크거나 같음), **~=** (비슷함)
- Value - 특성 데이터의 값을 정의합니다.

예: (&(city=Boston)(state=Massachusetts))

기본값: (objectclass=*)

동적 쿼리를 만들 때 다음 사항에 주의하십시오.

- "LDAP" 접두사는 다음과 같이 소문자여야 합니다.

  ldap:///o=MyCorporation??sub?(title=Manger)

- LDAP 서버 호스트 이름이나 포트 번호를 지정할 수 없습니다. 모든 검색은 사용자의 환경에 대해 구성한 LDAP 디렉터리 내에서 수행됩니다.

예: 예제 LDAP 쿼리

샘플 LDAP 쿼리는 다음과 같습니다.

설명	쿼리
관리자인 모든 사용자	ldap:///o=MyCorporation??sub?(title=Manger)
뉴욕 서부 지사에 있는 모든 관리자	ldap:///o=MyCorporation??one?(&(title=Manager) (office=NYWest))
휴대폰이 있는 모든 기술자	ldap:///o=MyCorporation??one? (&(employeetype=technician) (mobile=*))
사원 번호가 1000 - 2000 사이인 모든 사원	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
회사에서 6 개월 이상 근무한 모든 헬프 데스크 관리자	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22) **참고:** 이 쿼리를 사용하려면 사용자의 고용 날짜에 대해 DOH 특성을 만들어야 합니다.

참고: > 및 <(보다 큼 및 보다 작음) 비교는 산술적이 아니라 사전순입니다. 해당 사용에 대한 자세한 내용은 LDAP 디렉터리 서버 설명서를 참조하십시오.

그룹 구성원 수정

구성원 및 그룹을 추가 또는 제거하려면 이 옵션을 사용하십시오. 이 절차를 통해 구성원의 그룹 목록을 수정할 수 있습니다.

그룹 구성원을 수정하려면

1. 그룹 관리 권한이 있는 사용자로 CA Access Control 엔터프라이즈 관리에 로그인합니다.
2. "그룹", "그룹 구성원 수정"을 차례로 선택합니다.

   그룹 구성원 수정 화면이 나타납니다.
3. 그룹을 선택하고 "선택"을 클릭합니다.

   그룹 구성원 목록이 열립니다.
4. 구성원을 제거하려면 구성원 이름 옆의 확인란의 선택을 취소합니다.
5. 구성원을 추가하려면 "사용자 추가"를 클릭합니다.
   a. 검색 쿼리를 입력한 다음 "검색"을 클릭합니다.

      검색 조건에 따라 검색 쿼리 결과가 표시됩니다.
   b. 사용자를 선택하고 "선택"을 클릭합니다.

      사용자가 그룹 구성원으로 추가됩니다.
6. 그룹을 추가하려면 "그룹 추가" 단추를 클릭합니다.
   a. 검색 쿼리를 입력한 다음 "검색"을 클릭합니다.

      검색 조건에 따라 검색 쿼리 결과가 표시됩니다.
   b. 그룹을 선택하고 "선택"을 클릭합니다.

      그룹이 추가됩니다.
7. "제출"을 클릭합니다.

   작업이 성공적으로 완료되었음을 알리는 확인 메시지가 표시됩니다.

감사 데이터

감사 데이터는 CA Access Control 엔터프라이즈 관리 환경에서 발생하는 작업의 내역을 제공합니다. 감사 데이터의 예는 아래와 같습니다.

- 특정 기간에 대한 시스템 활동
- 특정 기간 중에 수정된 개체의 목록
- 사용자에게 할당된 역할
- 특정 사용자 계정에 대해 수행된 작업

감사 데이터는 이벤트에 대해 생성됩니다. 이벤트는 CA Access Control 엔터프라이즈 관리 작업에서 생성된 작업입니다. 예를 들어, "사용자 만들기" 작업은 AssignAccessRoleEvent 이벤트를 포함할 수 있습니다.

추가 정보:

제출된 작업 검색(페이지 41)
작업 상세 정보 보기(페이지 45)
이벤트 상세 정보 보기(페이지 45)

제출된 작업 검색

제출된 작업은 CA Access Control 엔터프라이즈 관리 환경의 작업에 대한 정보를 제공합니다. CA Access Control 엔터프라이즈 관리가 수행하는 작업에 대한 매우 자세한 정보를 검색하여 볼 수 있습니다. 세부 정보 화면은 각 작업과 이벤트에 대한 추가 정보를 제공합니다.

작업의 상태를 기반으로 작업을 취소하거나 다시 제출할 수 있습니다.

제출된 작업을 사용하여 시작부터 끝까지 작업의 처리를 추적할 수 있습니다.

제출한 작업을 검색하려면

1. CA Access Control 엔터프라이즈 관리에서 "시스템", "감사" 하위 탭을 차례로 클릭합니다.

   사용 가능한 작업 목록에 "제출된 작업 보기" 작업이 나타납니다.

2. "제출된 작업 보기"를 클릭합니다.

   "제출한 작업 보기" 페이지가 나타납니다.

3. 검색 조건(페이지 42)을 지정하고, 표시할 행 수를 입력한 다음 "검색"을 클릭합니다.

   검색 조건에 맞는 작업이 표시됩니다.

제출한 작업 보기의 검색 특성

처리를 위해 제출된 작업을 검토하려면 "제출한 작업 보기"의 검색 기능을 사용할 수 있습니다. 다음 조건을 기반으로 작업을 검색할 수 있습니다.

시작한 사람

작업을 시작한 사용자의 이름을 검색 조건으로 식별합니다. 사용자 이름을 기반으로 검색이 수행됩니다. 유효한 사용자 이름을 입력했는지 확인하려면 "유효성 검사" 단추를 사용합니다.

승인한 사람

작업 승인자의 이름을 검색 조건으로 식별합니다. 사용자 이름을 기반으로 검색이 수행됩니다. 유효한 사용자 이름을 입력했는지 확인하려면 "유효성 검사" 단추를 사용합니다.

참고: "다음에 의해 승인된 작업" 조건을 선택하여 작업을 필터링하는 경우 "승인 작업 표시" 조건도 기본적으로 활성화됩니다.

작업 이름

작업 이름을 검색 조건으로 식별합니다. 같음, 포함, 다음으로 시작 또는 다음으로 끝남과 같은 조건을 "작업 이름 위치" 필드 값과 함께 지정하여 검색을 구체화할 수 있습니다. 예를 들어, 같음 조건을 선택하고 텍스트 필드에 "사용자 만들기"를 입력하여 "작업 이름 같음 사용자 만들기"라는 검색 조건을 지정할 수 있습니다.

작업 상태

작업 상태(페이지 44)를 검색 조건으로 식별합니다. "작업 상태", 같음, 조건을 선택하여 작업 상태를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

- 완료함
- 진행 중
- 실패
- 거부됨
- 부분 완료됨
- 취소
- 예약됨

작업 우선 순위

작업 우선 순위를 검색 조건으로 식별합니다. "작업 우선 순위", 같음, 조건을 선택하여 작업 우선 순위를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

낮음

낮은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

중간

중간 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

높음

높은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

다음에서 수행됨

선택한 개체 인스턴스에서 수행된 작업을 식별합니다. 개체 인스턴스를 선택하지 않으면 해당 개체의 모든 인스턴스에서 수행된 작업이 표시됩니다.

참고: 이 필드는 "제출한 작업 구성" 화면의 "다음에서 수행됨 구성" 필드가 채워진 경우에만 나타납니다. 이 화면을 사용하여 "제출한 작업" 탭을 구성합니다.

날짜 범위

제출한 작업을 검색할 날짜 범위를 식별합니다. "시작 날짜" 및 "종료 날짜"를 제공해야 합니다.

제출되지 않은 작업 표시

"감사 마침" 상태의 작업을 식별합니다. 제출되지 않은 다른 작업을 시작한 작업을 식별합니다. 이 탭을 선택하면 이러한 작업이 모두 감사 및 표시됩니다.

승인 작업 표시

작업흐름의 일부로 승인되어야 하는 작업을 식별합니다.

추가 정보:

작업 상태 설명(페이지 44)

작업 상태 설명

제출한 작업은 아래에 설명된 상태 중 하나에 있습니다. 작업 상태를 기반으로 작업 취소 또는 작업 다시 제출과 같은 동작을 수행할 수 있습니다.

참고: 작업을 취소하거나 다시 제출하려면 작업 상태를 기반으로 취소 및 다시 제출 단추를 표시하도록 "제출한 작업 보기"를 구성해야 합니다.

진행 중

다음 중 하나가 발생하는 경우에 표시됩니다.

- 작업흐름이 시작되었지만 완료되지 않았음
- 현재 작업보다 먼저 시작된 작업이 진행 중임
- 중첩된 작업이 시작되었지만 완료되지 않았음
- 주 이벤트가 시작되었지만 완료되지 않았음
- 보조 이벤트가 시작되었지만 완료되지 않았음

이 상태의 작업은 취소할 수 있습니다.

참고: 작업을 취소하면 현재 작업의 불완전한 모든 중첩된 작업과 이벤트가 취소됩니다.

취소

진행 중인 작업이나 이벤트를 취소한 경우에 표시됩니다.

거부됨

CA Access Control 엔터프라이즈 관리가 작업흐름 프로세스의 일부인 이벤트나 작업을 거부하는 경우에 표시됩니다. 거부된 작업은 다시 제출할 수 있습니다.

참고: 작업을 다시 제출하면 CA Access Control 엔터프라이즈 관리는 실패 또는 거부한 중첩 작업과 이벤트를 모두 다시 제출합니다.

부분 완료됨

이벤트나 중첩된 작업 중 일부를 취소한 경우에 표시됩니다. 부분 완료된 이벤트나 중첩된 작업은 다시 제출할 수 있습니다.

완료함

작업이 완료된 경우에 표시됩니다. 현재 작업의 중첩된 작업 및 중첩된 이벤트가 완료되면 작업이 완료됩니다.

실패

작업, 중첩된 작업 또는 현재 작업에 중첩된 이벤트가 유효하지 않은 경우에 표시됩니다. 이 상태는 작업이 실패한 경우에 표시됩니다. 실패한 작업은 다시 제출할 수 있습니다.

예약됨

작업이 이후 날짜에 실행되도록 예약된 경우에 표시됩니다. 이 상태의 작업은 취소할 수 있습니다.

감사 마침

현재 작업이 감사된 경우에 표시됩니다.

작업 상세 정보 보기

CA Access Control 엔터프라이즈 관리는 제출된 작업의 상태, 중첩 작업, 작업 관련 이벤트와 같은 작업 상세 정보를 제공합니다.

제출한 작업의 상세 정보를 보려면

1. "제출된 작업 보기" 탭에서 선택한 작업 옆에 있는 오른쪽 화살표 아이콘을 클릭합니다.

   작업 상세 정보가 나타납니다.

   참고: 이벤트 및 중첩된 작업(있는 경우)이 "작업 상세 정보" 페이지에 표시됩니다. 각 작업 및 이벤트에 대해 작업 상세 정보를 볼 수 있습니다.

2. "닫기"를 클릭합니다.

   "작업 세부 정보" 탭이 닫히고 작업 목록이 포함된 "제출된 작업 보기" 탭이 CA Access Control 엔터프라이즈 관리에서 표시됩니다.

이벤트 상세 정보 보기

CA Access Control 엔터프라이즈 관리는 제출된 이벤트의 상태, 이벤트 특성, 이벤트에 대한 모든 추가 정보와 같은 이벤트 상세 정보를 제공합니다.

제출한 이벤트의 상세 정보를 보려면

1. "작업 상세 정보 보기" 페이지에서 이벤트 옆에 있는 오른쪽 화살표 아이콘을 클릭합니다.

   이벤트 상세 정보가 나타납니다.

2. "닫기"를 클릭합니다.

   "이벤트 상세 정보" 페이지가 닫힙니다.

제 3 장: 기업 구현 보기

이 장은 아래의 주제를 포함하고 있습니다.

월드 뷰

CA Access Control 엔터프라이즈 관리의 월드 뷰를 통해 연결된 DMS 에서 관리하고 있는 회사의 CA Access Control 구현을 볼 수 있습니다.

월드 뷰를 사용하여 다음을 수행할 수 있습니다.

- 연결된 DMS 에 보고하는 끝점을 식별합니다.
- CA Access Control, PMDB, PUPM, UNAB 중 하나인 끝점 유형을 식별합니다.
- 각 끝점에서 마지막으로 DMS 로 하트비트를 전송한 시간을 식별합니다.
- 배포된 정책, 운영 체제, 끝점에 있는 관리되는 장치와 같은 끝점에 대한 보다 자세한 정보를 봅니다.
- CA Access Control 끝점을 관리하기 위해 CA Access Control 끝점 관리를 엽니다.
- UNAB 호스트 또는 PUPM 관리되는 장치를 수정합니다.

회사의 CA Access Control 구현 보기

CA Access Control 엔터프라이즈 관리를 사용하여 회사의 CA Access Control 구현을 표시할 수 있습니다. 이 엔터프라이즈 "월드 뷰"는 모든 끝점, 끝점이 그룹화된 논리적 호스트 그룹, 끝점에 있는 배포된 정책, 끝점에 있는 관리되는 장치의 스냅숏입니다.

회사의 CA Access Control 구현을 보려면

1. CA Access Control 엔터프라이즈 관리에서 "월드 뷰" 탭을 클릭하고 왼쪽에 있는 작업 메뉴에서 "월드 뷰" 링크를 클릭합니다.

   "월드 뷰" 페이지가 나타나고 "검색" 섹션이 표시됩니다.

2. (선택 사항) 검색 조건을 정의합니다.

   다음과 같이 두 가지 검색 유형을 사용할 수 있습니다.

   - **단순** - 단순 검색을 사용하여 호스트 이름 마스크를 정의하고 결과를 필터링할 끝점의 유형을 지정합니다.
   - **고급** - "고급" 링크를 클릭하면 지정된 호스트 그룹, 할당된 정책, 관리되는 장치 이름 마스크, 관리되는 장치 유형을 기준으로 결과를 필터링할 수 있습니다.

   참고: 기본적으로 월드 뷰에는 CA Access Control 엔터프라이즈 관리가 연결되어 있는 DMS 에 정의된 모든 끝점에 대한 결과가 표시됩니다.

3. "실행"을 클릭합니다.

   다음 범주 중 하나로 정의한 조건과 일치하는 결과가 표시됩니다.

   - **호스트 이름별 결과** - DMS 에 정의하는 호스트(끝점)입니다. 이 범주는 결과를 표시할 때 사용되는 기본 범주입니다.
   - **호스트 그룹별 결과** - 정의하는 논리적 호스트 그룹입니다.
   - **정책별 결과** - 끝점에 배포된 정책입니다.
   - **관리되는 장치별 결과** - 끝점에 있는 관리되는 장치입니다.

CA Access Control 끝점 관리를 열어 끝점 관리

CA Access Control 엔터프라이즈 관리를 사용하면 CA Access Control 끝점 관리에 쉽게 로그인하여 CA Access Control 엔터프라이즈 관리가 관리하는 모든 끝점을 관리할 수 있습니다.

CA Access Control 이 사용자를 끝점에 자동으로 로그인하도록 하려면 CA Access Control 엔터프라이즈 관리와 동일한 사용자 이름과 암호를 사용하고 있는지 확인하고, CA Access Control 끝점 관리를 사용하여 끝점을 관리하기 위한 터미널 액세스 권한이 CA Access Control 끝점 관리에 있는지 확인하십시오.

CA Access Control 끝점 관리를 열어 끝점을 관리하려면

1. 월드 뷰를 사용하여 관리할 끝점 하나 이상을 표시합니다.
2. "작업" 열에서 "관리"를 클릭합니다.

   CA Access Control 끝점 관리가 열리고 끝점의 호스트 이름과 사용자의 자격 증명이 자동으로 입력됩니다. 로그인하는 데 사용한 CA Access Control 엔터프라이즈 관리 사용자 계정이 CA Access Control 끝점 관리에 없으면 자격 증명을 직접 입력해야 합니다.

추가 정보:

회사의 CA Access Control 구현 보기(페이지 48)

PUPM 끝점 수정

CA Access Control 엔터프라이즈 관리 월드 뷰를 사용하여 PUPM 끝점의 관리되는 장치에 대한 설정을 수정할 수 있습니다. 관리되는 장치는 권한 있는 계정을 사용하여 관리하는 응용 프로그램입니다. PUPM 끝점은 계정에 대한 액세스를 부여하는 역할 기반 관리 시스템을 사용하여 권한 있는 계정을 암호 데이터베이스에 저장합니다. 관리되는 장치는 PUPM 끝점 자체에 설치되거나 엔터프라이즈에 설치할 수 있습니다.

PUPM 끝점을 수정하려면

1. "월드 뷰", "월드 뷰" 작업을 차례로 선택합니다.
   월드 뷰 검색 화면이 나타납니다.
2. 쿼리를 입력한 다음 "실행"을 클릭합니다.
   쿼리에 대한 검색 결과가 표시됩니다.
3. "보기" 옵션을 선택하여 수정할 PUPM 끝점을 선택합니다.
   풀다운 메뉴에 끝점에 있는 관리되는 장치가 표시됩니다.
4. "수정"을 클릭하여 끝점 설정을 수정합니다.
   끝점 수정 창이 나타나고 여기에 끝점 설정이 표시됩니다.
5. 끝점 설정을 수정하고 "제출"을 클릭합니다.
   작업이 완료되었음을 알리는 메시지가 표시됩니다.

제 4 장: 중앙에서 정책 관리

이 장은 아래의 주제를 포함하고 있습니다.

정책 유형

CA Access Control 엔터프라이즈 관리에서는 CA Access Control 정책, UNAB 구성 정책, UNAB 로그인 정책의 세 가지 정책 유형을 사용하여 CA Access Control 끝점 및 UNAB 호스트를 관리합니다.

CA Access Control 정책은 회사 전체에서 CA Access Control 끝점에 대한 접근자의 권한을 설정하고 리소스에 대한 액세스를 제어하기 위한 통일된 정책을 만들 때 사용합니다.

UNAB 로그인 정책은 회사 내의 UNIX 호스트에 대한 액세스를 관리할 때 사용합니다. 로그인 정책은 UNAB 가 실행되는 UNIX 호스트에 대한 사용자의 로그인을 제어합니다. CA Access Control 엔터프라이즈 관리는 전파한 권한 부여 목록을 기반으로 자동으로 로그인 정책을 만들고, 할당하고, 배포합니다.

UNAB 구성 정책은 조직 내에서 UNAB 호스트를 배포 및 구성하기 위해 원격 UNAB 호스트의 구성 파일에 있는 토큰 값을 설정할 때 사용합니다.

이 장은 CA Access Control 정책 사용법을 설명합니다.

추가 정보:

UNAB 로그인 권한 부여 관리(페이지 139)
UNAB 호스트 또는 호스트 그룹 구성(페이지 141)

중앙에서 정책을 관리하기 위한 방법

CA Access Control 을 사용하면 다음 방법으로 단일 컴퓨터에서 여러 데이터베이스를 관리할 수 있습니다.

- **자동 규칙 기반 정책 업데이트** - 중앙 데이터베이스(PMDB)에서 정의한 일반 규칙은 구성된 계층의 데이터베이스에 자동으로 전파됩니다.

  참고: 이중 제어는 이 방법으로만, UNIX 에서만 사용할 수 있습니다. 자동 규칙 기반 정책 업데이트의 이중 제어에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오. 자동 규칙 기반 정책 업데이트에 대한 자세한 내용은 Windows 용 끝점 관리 안내서를 참조하십시오.

- **고급 정책 관리** - 사용자가 배포하는 정책(규칙 그룹)은 호스트 또는 호스트 그룹 할당에 따라 모든 데이터베이스에 전파됩니다. 정책을 배포 취소(제거)하고 배포 상태와 배포 위반을 확인할 수도 있습니다. 이 기능을 사용하려면 추가 구성 요소를 설치하고 구성해야 합니다.

  참고: 고급 정책 관리에 대한 자세한 내용은 엔터프라이즈 관리 안내서를 참조하십시오.

고급 정책 관리

여러 규칙 정책(selang 명령)을 작성하여 저장한 후, 사용자가 정의하는 방식으로 기업에 배포할 수 있습니다. 이 정책 기반 방법을 사용하여 정책을 저장한 다음 호스트 또는 그룹 호스트에 할당할 수 있습니다. 할당된 정책은 배포를 위해 큐에 추가됩니다. 또는 호스트나 그룹 호스트에 직접 정책 버전을 배포 및 배포 취소할 수 있습니다.

중앙 데이터베이스인 DMS(Deployment Map Server)에서는 기업 정책, 버전, 할당 및 배포에 대한 모든 정보를 수집합니다. 따라서 배포 상태, 배포 위반 및 배포 계층에 대해 쉽게 보고할 수 있습니다.

참고: 이중 제어는 이 방법에서 사용할 수 없으며 UNIX 에서만 사용할 수 있습니다. 자세한 내용은 UNIX 용 끝점 관리 안내서를 참조하십시오.

고급 정책 기반 관리 작동 방법

고급 정책 기반 관리를 통해 정책 버전을 저장, 배포 및 배포 취소하고 나중에 배포 상태, 배포 위반 및 배포 분산을 확인할 수 있습니다.

고급 정책 기반 관리는 다음 방식으로 작동합니다.

1. 정책을 만듭니다.

   각 정책은 selang 명령 스크립트 쌍을 포함합니다. 첫 번째 스크립트는 배포 스크립트이며 정책을 구성하는 selang 명령 집합이 포함되어 있습니다. 두 번째 스크립트는 배포 취소 스크립트라고 하며 끝점 데이터베이스에서 정책의 배포를 취소(제거)하는 데 필요한 명령을 포함하고 있습니다.

2. CA Access Control 엔터프라이즈 관리 또는 policydeploy 유틸리티를 사용하여 DMS 에 정책 세부 정보를 저장하면 CA Access Control 은 자동 버전 제어 기능을 사용하여 정책을 저장합니다.

   정책 세부 정보에는 정책 설명, 배포/배포 취소 스크립트, 정책 종속성이 포함됩니다.

3. DMS 에 정책이 이미 있는지 여부에 따라 CA Access Control 은 다음 중 하나를 수행합니다.

   - DMS 에 정책 이름이 없으면 CA Access Control 은 정책의 첫 번째 버전(policy_name#01)과 논리적 정책 개체(GPOLICY 클래스)를 만든 다음 정책 버전을 논리적 정책의 구성원으로 추가합니다.
   - DMS 에 정책 이름이 이미 있으면 CA Access Control 은 검색된 가장 높은 정책 버전에 한 버전을 증가시켜 새 정책 버전을 만들고 이 정책 버전을 논리적 정책(GPOLICY 개체)의 구성원으로 추가합니다.

4. 준비가 되었다고 판단되면 CA Access Control 엔터프라이즈 관리나 policydeploy 유틸리티를 사용하여 저장된 정책을 대상 데이터베이스에 배포합니다. CA Access Control 은 DMS 에서 자동으로 배포 작업(DEPLOYMENT 개체)를 만듭니다.

   참고: CA Access Control 은 저장된 정책의 최종 완료된 정책 버전을 배포합니다. 만드는 새 정책 버전은 자동으로 할당된 호스트에 전달되지 않습니다. 할당된 호스트를 최신 정책 버전으로 수동으로 업그레이드해야 합니다.

   참고: 정책을 만든 이후에 CA Access Control 엔터프라이즈 관리는 UNAB 로그인 및 프로시저 정책을 자동으로 배포합니다. 사용자는 UNAB 로그인 및 구성 정책만 UNAB 호스트에 할당할 수 있습니다.

5. CA Access Control 은 DMS 에서 배포 패키지(GDEPLOYMENT 개체)를 자동으로 만듭니다.

   배포 패키지는 이전 단계에서 작성된 모든 배포 작업을 그룹화합니다.

6. DMS 가 배포 작업을 DH(배포 호스트)로 보냅니다.
7. 끝점은 policyfetcher 를 통해 새 정책 배포 작업이 있는지 정기적으로 확인하여 DH 에서 보류 중인 배포 작업을 가져오고 각 규칙(배포 스크립트에 지정된 selang 명령)을 대상 데이터베이스에서 실행합니다.
8. 끝점은 DH 에서 배포 작업 상태(실패/성공), 실패한 명령에 대한 selang 결과 메시지, HNODE 의 정책 상태를 업데이트합니다.

   참고: 정책을 배포할 때 오류가 발생하면 CA Access Control 엔터프라이즈 관리의 배포 감사를 사용하여 실패한 명령에 대한 자세한 selang 출력을 볼 수 있습니다. 또는 정책을 배포할 때 오류가 발생한 컴퓨터에서 로그 파일을 확인해야 할 수도 있습니다.
9. DH 가 이 정보가 저장된 DMS 에서 배포 작업 상태와 정책 상태를 업데이트합니다.

참고: UNAB 로그인 정책 및 UNAB 구성 정책은 고급 정책 기반 관리와 같은 방식으로 작동하지 않습니다.

추가 정보:

정책 종속성(페이지 66)
정책 확인(페이지 67)
할당 경로(페이지 63)
호스트 액세스를 제어하고 UNAB 를 구성하는 방법(페이지 139)

배포 방법이 배포 작업에 주는 영향

저장된 정책을 대상 데이터베이스로 배포할 때 CA Access Control 은 DMS 에 배포 작업을 자동으로 만듭니다. 배포 작업(DEPLOYMENT 개체)은 끝점에서 실행할 작업 지시로서 DMS 에서 생성됩니다. 각 배포 작업은 한 끝점에만 사용되며 끝점에 배포하는 데 필요한 정책 버전 정보를 포함하고 있습니다.

참고: CA Access Control 은 다른 배포 방법을 사용하여 UNAB 로그인 및 구성 정책을 배포합니다.

저장된 정책을 배포하기 위해 사용하는 방법은 CA Access Control 이 만드는 배포 작업에 영향을 줍니다. 다음은 다른 방법을 선택할 때의 결과에 대해 설명합니다.

- 정책(GPOLICY 개체)을 하나 이상의 호스트에 할당

  CA Access Control 은 호스트별로 정책의 최종 완료된 버전에 대한 배포 작업을 만듭니다.

- 정책(GPOLICY 개체)을 하나 이상의 호스트 그룹에 할당

  CA Access Control 은 호스트 그룹 중 하나의 구성원인 호스트별로 정책의 최종 완료된 버전에 대한 배포 작업을 만듭니다.

- 저장된 정책(GPOLICY 개체)이 할당된 호스트 그룹에 호스트 추가

  CA Access Control 은 새 호스트에 대해 정책의 최종 완료된 버전에 대한 배포 작업을 만듭니다.

- 정책을 하나 이상의 호스트에 재배포

  CA Access Control 은 호스트별로 정책의 최종 완료된 버전에 대한 배포 작업을 만듭니다.

- HNODE 에서 정책 복원(호스트에 배포해야 하는 정책 재배포)

  CA Access Control 은 호스트에 배포해야 하는 정책별로 해당 호스트에서 유효한 정책 버전에 대한 배포 작업을 만듭니다.

- 하나 이상의 호스트에서 배포된 정책 업그레이드

  호스트에 저장된 버전이 호스트에 배포된 것보다 최신 버전인 경우 CA Access Control 은 호스트별로 최종 완료된 정책 버전에 대한 배포 작업을 만듭니다.

예: 호스트에 정책 할당

정책 IIS 를 호스트 host1.comp.com 및 host2.comp.com 에 할당하는 경우 CA Access Control 은 최신 IIS 정책 버전을 host1.comp.com 에 배포하기 위한 작업과 최신 IIS 정책 버전을 host2.comp.com 에 배포하기 위한 작업의 두 가지 배포 작업을 만듭니다.

예: 호스트 그룹에 정책 할당

호스트 그룹 서버에 hostA.comp.com 및 hostB.comp.com 의 두 개의 구성원이 있습니다. 정책 IIS 를 호스트 그룹 서버에 할당하는 경우 CA Access Control 은 최신 IIS 정책 버전을 hostA.comp.com 및 hostB.comp.com 에 배포하는 각각 두 개의 배포 작업을 만듭니다.

예: 할당된 정책이 있는 호스트 그룹에 호스트 추가

호스트 그룹 서버에는 두 개의 할당된 정책(IIS 및 ORACLE)이 있습니다. 호스트 test.comp.com 을 호스트 그룹에 추가하는 경우 CA Access Control 은 최신 IIS 정책 버전을 test.comp.com 에 배포하는 작업과 최신 ORACLE 정책 버전을 test.comp.com 에 배포하는 두 가지 배포 작업을 만듭니다.

예: 호스트 복원

호스트에 policy1 과 policy2 의 두 개의 할당된 정책이 있습니다. 호스트를 복원하는 경우 CA Access Control 은 호스트에서 최종 완료된 policy1 버전을 배포하는 작업과 최종 완료된 policy2 버전을 배포하는 두 가지 배포 작업을 만듭니다.

예: 배포된 정책 업그레이드

정책 IIS 가 host1.comp.com 및 host2.comp.com 의 두 개 호스트에 배포되었지만 정책 IIS 의 최종 버전은 host1.comp.com 에 배포되지 않았습니다. 두 호스트 모두에서 정책 IIS 를 업그레이드하는 경우 CA Access Control 은 최신 IIS 정책 버전을 host1.comp.com 에 배포하는 하나의 배포 작업만 만듭니다.

추가 정보:

호스트 액세스를 제어하고 UNAB 를 구성하는 방법(페이지 139)

DMS 가 수록한 끝점 데이터

회사 환경에 고급 정책 관리를 구성할 때 회사의 끝점은 구성된 DH 를 통해 다음 세 가지 영역의 상태 변경 사항을 DMS 에 통보합니다.

- 정책 배포 및 배포 취소

  정책이 배포 또는 배포 취소될 때 끝점은 알림을 보냅니다. 그러면 작업 결과에 따라 다음 세부 정보가 업데이트됩니다.

  - 정책 세부 정보
  - 배포 상태(성공, 실패 등)
  - 실행하지 못한 정책 명령의 selang 명령 출력
  - HNODE 정책 상태(배포됨, 배포 실패 등)

- 호스트 하트비트

  일반 구성 가능한 간격으로 각 끝점은 온라인 상태의 호스트에 대한 계정으로 하트비트를 전달합니다.

- 위반 상태

  각 하트비트 이후에 끝점은 정책 위반을 계산하여 그 결과(위반 발견 여부)를 보냅니다. policyfetcher 가 끝점과 DH 사이에 배포 및 위반 상태 충돌을 발견하면 끝점 정보에 기초하여 이러한 충돌을 해결합니다.

끝점이 DMS 를 업데이트하는 방법

각 끝점은 구성한 DH 를 통해 DMS 로 하트비트(호스트 상태), 정책 상태, 위반 상태 알림을 보냅니다. 해당 DMA 알림은 다음과 같은 방법으로 처리됩니다.

1. DH 가 업데이트 파일에 알림 메시지를 저장합니다.

   이러한 알림은 끝점에서 보내는 하트비트 및 정책 배포/배포 취소 알림입니다.

2. DH 에서 구독자인 DMS 에 연결합니다.
   - DMS 를 사용할 수 없는 경우 DH 는 모든 메시지를 성공적으로 보낼 때까지 정기적으로 DMS 와 통신하려고 시도합니다.
   - DMS 를 사용할 수 있는 경우 DH 는 저장된 알림을 보냅니다.
3. DMS 가 나중에 사용할 수 있도록 각 DH 에서 받은 정보를 저장합니다.

   보고서를 작성할 때마다 CA Access Control 에서는 DMS 의 정보를 검색합니다.

참고: UNAB 끝점은 다른 프로세스를 사용하여 DMS 를 업데이트합니다.

추가 정보:

호스트 액세스를 제어하고 UNAB 를 구성하는 방법(페이지 139)

고급 정책 관리 클래스

CA Access Control 은 특수 클래스를 사용하여 DMS 에서 다음을 가능하게 합니다.

- 각 컴퓨터에 배포된 정책 상태의 최신 맵을 유지합니다.
- 끝점이 포함해야 할 관련 정책 배포 정보를 끝점이 가져올 수 있도록 DH 에 배포 정보를 보냅니다.

참고: 이러한 클래스가 허용하는 속성에 대한 자세한 내용은 selang 참조 안내서를 참조하십시오.

DEPLOYMENT 클래스

DEPLOYMENT 클래스의 각 개체는 정책 배포 작업을 나타냅니다. CA Access Control 에서는 사용자가 호스트에 정책을 할당 또는 할당 취소하거나 정책을 직접 배포 또는 배포 취소할 때 DMS 에서 배포 작업을 자동으로 작성합니다. 사용자가 정책이 할당된 호스트 그룹에서 호스트를 추가(할당) 또는 제거(할당 취소)하고, 호스트에서 정책을 다운그레이드 또는 업그레이드하고, 호스트를 재설정 또는 복원할 때에도 배포 작업이 작성됩니다.

끝점은 이 개체를 작업 지시로 사용하여 보류 중인 DEPLOYMENT 개체의 정보에 따라 정책 버전을 배포 또는 배포 취소합니다. 각 작업 지시는 한 끝점에만 사용되며 끝점에 배포하는 데 필요한 정책 버전 정보를 포함하고 있습니다. 또한 DEPLOYMENT 개체에는 배포의 성공 여부를 나타내는 상태 속성과 정책 배포 작업의 selang 명령 출력이 포함된 결과 속성(result_message)이 있습니다.

참고: 다른 할당 경로로 인해 HNODE 에 이미 정책이 있는 경우에는 배포 작업이 비어 있을 수 있습니다(작업 없음 상태).

GDEPLOYMENT 클래스

GDEPLOYMENT 클래스의 각 개체는 배포 패키지를 나타냅니다. 배포 패키지는 동일한 트랜잭션(정책 할당, 업그레이드 등)의 결과로 특정 호스트에 대해 작성되는 모든 배포 작업과 함께 DMS 및 그룹에 자동으로 작성됩니다. 즉, 사용자가 만드는 각 트랜잭션은 필요한 수만큼의 배포 작업을 생성하며(DEPLOYMENT 개체) 이들을 호스트별로 그룹화합니다(GDEPLOYMENT 개체).

배포 패키지는 정책 배포를 추적하고 문제를 해결할 수 있게 해주며 배포가 시작된 이유인 트리거를 기록합니다.

HNODE 클래스

HNODE 클래스의 각 개체는 회사 내에 있는 각 끝점을 나타냅니다. 이 개체에는 개체가 나타내는 특정 노드, 개체가 속한 호스트 그룹 및 개체가 마지막으로 온라인에서 검색된 시간에 대한 정보가 포함되어 있습니다. 또한 각 HNODE 개체에는 개체가 직접 또는 간접 할당을 통해 나타내는 노드에서 유효한 정책 버전과 각 정책의 상태(배포됨, 배포되었지만 오류 발생 등)에 대한 정보가 포함되어 있습니다.

HNODE 개체 이름은 실제 호스트 이름입니다. 예: myhost.mydomain.com

GHNODE 클래스

GHNODE 클래스의 각 개체는 CA Access Control 노드(HNODE 개체)의 그룹을 나타냅니다. 이 개체를 사용하면 정책을 배포하기 위해 끝점을 논리적 그룹으로 그룹화할 수 있습니다. 각 GHNODE 개체에는 개체가 나타내는 노드에 할당된 정책에 대한 정보가 포함되어 있습니다.

POLICY 클래스

POLICY 클래스의 각 개체는 호스트(HNODE 개체) 또는 호스트의 논리적 그룹(GHNODE 개체)에 배포할 수 있는 정책(GPOLICY 개체)의 버전을 나타냅니다. 이 개체에는 연관된 정책 스크립트가 저장되어 있는 위치(RULESET 개체) 및 개체를 배포해야 하는 노드 또는 노드 그룹에 대한 정보가 포함되어 있습니다.

이 개체의 이름은 정책 이름이며 버전 번호가 접미사로 사용됩니다(policy_name#xx).

GPOLICY 클래스

GPOLICY 클래스의 각 개체는 논리 정책을 나타냅니다. 이 개체에는 이 정책에 속한 정책 버전(POLICY 개체)과 개체가 할당된 호스트 및 호스트 그룹에 대한 정보가 포함되어 있습니다.

이 개체의 이름은 논리 정책 이름입니다.

RULESET 클래스

RULESET 클래스의 각 개체에는 정책 버전과 연관된 배포 스크립트와 배포 취소(제거) 스크립트가 모두 포함되어 있습니다.

이 개체의 이름은 각 POLICY 개체 이름에 따라 다릅니다.

호스트 및 호스트 그룹

고급 정책 관리를 사용하려면 기업의 CA Access Control 구현을 정의해야 합니다. 이렇게 하려면 끝점이나 호스트를 나타내는 HNODE 개체와 논리 호스트 그룹을 나타내는 GHNODE 개체를 작성합니다. 호스트는 해당 속성과 정책 요구에 따라 여러 논리 호스트 그룹의 구성원이 될 수 있습니다. 예를 들어 호스트에서 Red Hat 운영 체제와 Oracle 을 실행하는 경우 호스트는 기본 Red Hat 액세스 제어 정책을 가져오기 위한 Red Hat 논리 호스트 그룹의 구성원인 동시에 Oracle 액세스 제어 정책을 가져오기 위한 Oracle 논리 호스트 그룹의 구성원이 될 수 있습니다.

끝점을 기업의 호스트로 정의

끝점에 정책을 배포하고 해당 배포 상태를 표시하려면 DMS(Deployment Map Server)에서 기업 관리에 사용되는 끝점을 정의해야 합니다. 고급 정책 관리가 활성화되었을 때 끝점에 CA Access Control 을 설치하면 해당 끝점을 나타내는 HNODE 레코드가 자동으로 DMS 에 생성됩니다. 끝점에 CA Access Control 을 설치하기 전에 환경을 모델링하려는 경우에만 DMS 에서 끝점을 직접 정의해야 합니다.

중요! HNODE 이름에는 정규화된 호스트 이름을 사용해야 합니다. 그렇지 않으면 끝점이 배포를 수집하지 않습니다.

끝점을 기업의 호스트로 정의하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "호스트" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "호스트" 트리를 확장합니다.

   사용 가능한 작업 목록에 "호스트 만들기" 작업이 나타납니다.

2. "호스트 만들기"를 클릭합니다.

   "호스트 만들기: 호스트 검색" 화면이 나타납니다.

3. "호스트" 유형의 새 개체 만들기가 선택되었는지 확인하고 "확인"을 클릭합니다.

   "호스트 만들기" 작업 페이지가 나타납니다.

4. 대화 상자에서 다음 필드를 채웁니다.

   이름

   끝점(HNODE 개체)의 이름을 정의합니다. 이 이름은 DMS 에서 고유해야 합니다(필수).

   설명

   (선택 사항) 호스트의 비즈니스 설명(자유 텍스트)을 정의합니다. 이 필드를 사용하여 끝점을 식별하는 데 도움이 되는 정보를 기록하십시오.

   IP 주소

   (선택 사항) 호스트의 IP 주소를 정의합니다.

5. "제출"을 클릭합니다.

   작업이 성공적으로 제출되면 새 호스트(HNODE)가 만들어졌음을 알리는 메시지가 바로 나타납니다.

논리 호스트 그룹 정의

관련 끝점 그룹에서 정책을 관리하려면 끝점을 논리 호스트 그룹으로 정의하고 전체 그룹에서 고급 정책 관리 작업을 수행하십시오. 의미 있는 호스트 그룹을 작성하려면 먼저 DMS 에서 끝점을 정의해야 합니다.

참고: 이 절차에서는 CA Access Control 엔터프라이즈 관리를 사용하여 DMS 에서 논리 호스트 그룹을 정의하는 방법에 대해 설명합니다.

논리 호스트 그룹을 정의하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "호스트" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "호스트 그룹" 트리를 확장합니다.

   사용 가능한 작업 목록에 "호스트 그룹 만들기"가 나타납니다.

2. "호스트 그룹 만들기"를 클릭합니다.

   "호스트 그룹 만들기: 호스트 그룹 검색" 화면이 나타납니다.

3. "호스트 그룹" 유형의 새 개체 만들기가 선택되었는지 확인하고 "확인"을 클릭합니다.

   "호스트 그룹 만들기" 작업 페이지가 나타납니다.

4. 대화 상자에서 다음 필드를 채웁니다.

   이름

   논리 호스트 그룹(GHNODE 개체)의 이름을 정의합니다.

   설명

   (선택 사항) 호스트 그룹의 비즈니스 설명(자유 텍스트)을 정의합니다. 이 필드를 사용하여 호스트 그룹을 식별하는 데 도움이 되는 정보를 기록하십시오.

5. "호스트 선택"을 클릭한 다음 "추가"를 클릭합니다.

   "구성원 추가" 대화 상자가 나타납니다.

6. 호스트 그룹에 추가할 끝점을 선택하고 "선택"을 클릭합니다.

   "구성원 추가" 대화 상자가 닫히고 선택한 끝점이 정의 중인 논리적 그룹 호스트의 "구성원 목록"에 추가됩니다.

7. "제출"을 클릭합니다.

   작업이 성공적으로 제출되면 새 그룹 호스트(GHNODE)가 만들어졌음을 알리는 메시지가 바로 나타납니다.

호스트 그룹 가져오기

호스트 그룹을 가져오면 기존 PMDB 구조를 고급 정책 관리로 마이그레이션하는 데 도움이 됩니다. 호스트 그룹을 가져올 때는 호스트 그룹에 호스트를 만들거나 호스트를 조인합니다. 호스트는 PMDB 의 구독자에 해당합니다.

참고: 고급 정책 관리는 계층적 호스트 그룹을 지원하지 않습니다. PMDB 에서 호스트 그룹을 가져올 때는 모든 구독자의 계층을 동일한 호스트 그룹으로 단일화합니다. CA Access Control 엔터프라이즈 관리는 구독자 PMDB 에 해당하는 호스트를 만들지 않습니다.

호스트 그룹에 조인하는 각 PMDB 구독자에 대해 CA Access Control 엔터프라이즈 관리는 구독자에 해당하는 호스트(HNODE 개체)가 이미 DMS 에 있는지 여부를 확인합니다. 해당 호스트가 DMS 에 있으면 CA Access Control 은 이 호스트를 호스트 그룹에 추가합니다. 해당 호스트가 DMS 에 없으면 CA Access Control 은 새 호스트를 만들어 호스트 그룹에 추가합니다.

액세스 권한이 없는 끝점은 마법사에 표시되지 않으며 해당 호스트를 호스트 그룹에 추가할 수 없습니다.

호스트 그룹을 가져오려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "정책 관리"를 클릭합니다.
   b. "호스트" 하위 탭을 클릭합니다.
   c. 작업 메뉴에서 왼쪽에 있는 "호스트 그룹" 트리를 확장합니다.

      사용 가능한 작업 목록에 "호스트 그룹 가져오기" 작업이 나타납니다.
2. "호스트 그룹 가져오기"를 클릭합니다.

   PMDB 호스트 로그인 페이지가 나타납니다.
3. 사용자 이름, 암호, PMDB 이름을 입력한 다음 "로그인"을 클릭합니다.

   참고: master_pmdb@example 과 같이 PMDBname@host 형식으로 PMDB 이름을 지정하십시오.

   "일반" 작업 단계에 "호스트 그룹 가져오기" 마법사가 나타납니다.

4. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.

   CA Access Control 이 호스트를 호스트 그룹에 추가합니다. DMS 에 호스트가 없으면 CA Access Control 은 호스트를 호스트 그룹(GHNODE)에 추가하기 전에 호스트에 대한 HNODE 개체를 만듭니다.

   참고: 호스트를 기존 호스트 그룹에 추가하면 CA Access Control 은 호스트 그룹에 할당된 모든 정책을 이 호스트에 자동으로 배포합니다.

할당 경로

할당 경로는 특정 호스트나 호스트 그룹에 대한 정책 할당을 설명합니다. 정책은 다음과 같은 두 가지 경로로 호스트에 할당할 수 있습니다.

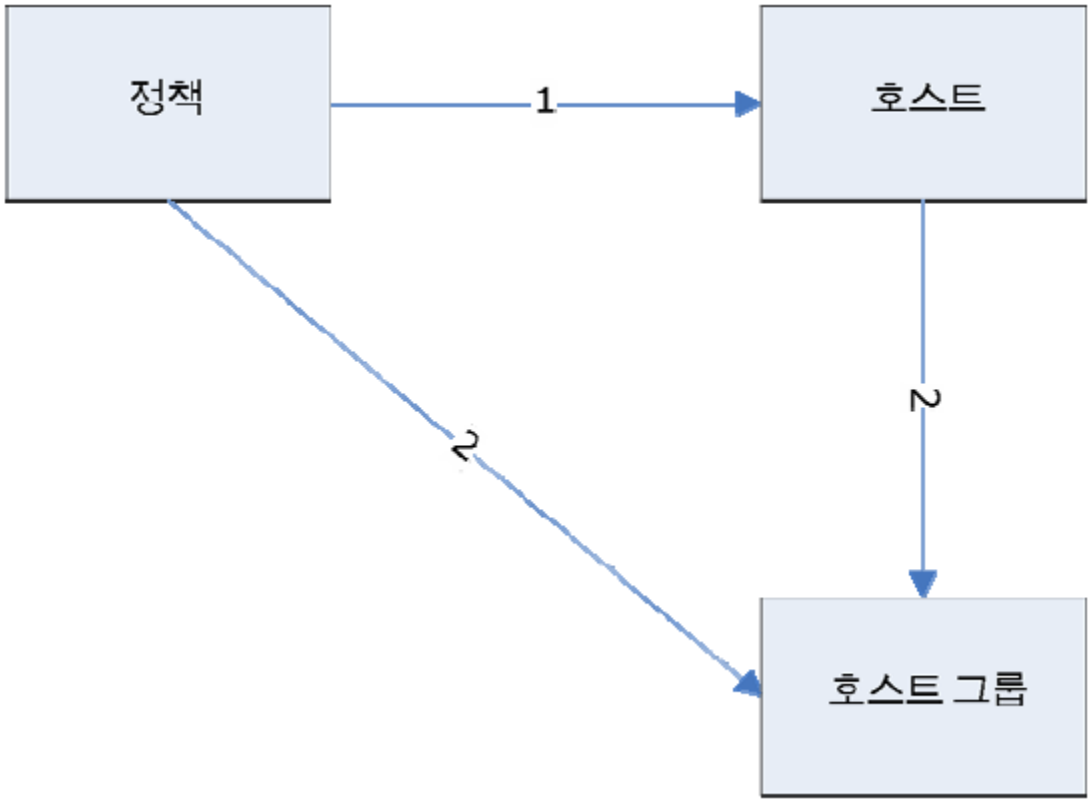
- 정책이 호스트에 직접 할당됩니다.
- 정책이 호스트가 구성원인 호스트 그룹에 할당됩니다.
- 호스트가 하나 이상의 정책이 할당된 호스트 그룹에 조인됩니다.

할당 경로는 여러 개일 경우 다음과 같이 고급 정책 관리에 영향을 미치기 때문에 중요합니다.

- 할당 경로를 하나 제거해도 호스트와 정책 사이에 다른 할당 경로가 있기 때문에 CA Access Control 이 정책을 배포 취소하지 않습니다.
- 할당 경로를 추가하면 추적 및 관리 용도로 배포 패키지와 배포 작업이 생성됩니다. 그러나 배포 작업의 상태는 작업 없음이므로 끝점에서 정책 배포가 시작되지 않습니다.

예: 정책 IIS 에 대한 다중 할당 경로

다음 그림은 정책 IIS 에 대한 다중 할당 경로의 예를 설명합니다. 호스트 host1.comp.com 은 호스트 그룹 "Servers"의 구성원입니다. 경로 1 은 정책 IIS 를 호스트 host1.comp.com 에 직접 할당할 때의 할당 경로입니다. 경로 2 는 정책 IIS 를 호스트 그룹 "Servers"에 할당할 때의 할당 경로입니다.



예: 할당 경로 제거

앞의 그림에서 정책 IIS 는 호스트 그룹 "Servers" 및 호스트 host1.comp.com 에 할당되었습니다. "Servers" 호스트 그룹에서 host1.comp.com 을 제거하면 경로 2 가 제거됩니다. 하지만 CA Access Control 은 정책 IIS 가 아직 호스트(경로 1)에 직접 할당되어 있으므로 host1.comp.com 에서 정책 IIS 를 배포 취소하지 않습니다.

정책 생성 및 배포 방법

고급 정책 기반 관리를 사용하여 정책의 초안 버전을 저장하고 필요에 따라 검토 및 수정한 다음 승인된 버전을 배포할 수 있습니다.

CA Access Control 엔터프라이즈 관리를 사용하여 승인된 정책 버전을 배포하려면 다음 작업을 수행합니다.

1. 정책 버전을 DMS 에 저장합니다.

   정책 버전을 저장한 다음 정책을 검토하고 배포할 수 있습니다.

2. 정책을 검토합니다.

   정책 버전이 저장된 이후에는 검토한 정책과 관련된 규칙이 있어야 합니다.

3. 정책을 완료합니다.

   정책을 완료한 후에는 정책을 배포할 호스트 및 호스트 그룹에 정책을 할당할 수 있습니다.

4. 다음과 같은 사용 가능한 경로 중 하나를 통해 끝점에 정책을 할당합니다.

   - 저장된 정책을 호스트 또는 호스트 그룹에 할당합니다.
   - 이미 정책이 할당된 호스트의 논리적 그룹에 호스트를 할당합니다.

   정책이 할당되면 CA Access Control 은 정책의 최종 완료된 버전을 자동으로 배포합니다.

참고: UNAB 로그인과 구성 정책을 만들고 배포하려면 다른 프로세스를 따르십시오.

추가 정보:

UNAB 로그인 권한 부여 관리(페이지 139)
UNAB 호스트 또는 호스트 그룹 구성(페이지 141)
할당 경로(페이지 63)

관리 요구 사항

DMS 에 정책을 저장하거나 이러한 정책을 할당하려면 사용자 및 사용자가 작업 중인 컴퓨터에 적절한 사용 권한이 있어야 합니다.

DMS 에 정책을 저장하려면

- DMS 를 관리하고 있는 컴퓨터나 policydeploy 유틸리티를 실행하고 있는 컴퓨터에 DMS 에 대한 터미널 권한(TERMINAL 클래스)이 있어야 합니다.
- 사용자는 DMS 의 POLICY, GPOLICY 및 RULESET 클래스에 대해 하위 관리 권한이 있어야 합니다.

호스트 또는 호스트 그룹에 정책을 할당하려면:

- DMS 를 관리하는 데 사용하는 컴퓨터에 DMS 에 대한 터미널 권한(TERMINAL 클래스)이 있어야 합니다.
- 사용자는 DMS 의 DEPLOYMENT, GDEPLOYMENT, POLICY, GPOLICY, HNODE 및 GHNODE(호스트 그룹에 정책을 할당하는 경우) 클래스에 대해 하위 관리 권한이 있어야 합니다.

참고: 터미널 권한 및 하위 관리 권한에 대한 자세한 내용은 UNIX 용 끝점 관리 안내서 및 Windows 용 끝점 관리 안내서를 참조하십시오.

정책 종속성

고급 정책 관리를 사용하면 정책이 배포 또는 배포 취소되는 순서를 적용할 수 있습니다.

정책 종속성을 사용하면 하나 이상의 다른 정책에 종속된 정책이 필수 정책이 배포될 때까지 배포되지 않도록 정의할 수 있습니다. 마찬가지로 의존적인 정책이 하나 이상 배포되어 있는 경우에는 필수 구성 요소 정책을 배포 취소할 수 없습니다.

정책을 만들거나 수정할 때 정책 종속성을 정의합니다.

정책 확인

정책 확인이 활성화되면 CA Access Control 은 정책을 배포하기 전에 정책에 오류가 없는지 검사합니다. CA Access Control 이 정책 배포 스크립트에서 오류를 발견하면 이 정책 스크립트는 끝점에서 실행되지 않습니다. 이렇게 하면 오류 있는 정책이 배포되지 않고 끝점에서 스크립트 오류를 추적할 수 있게 됩니다. 정책 확인은 기본적으로 비활성화되어 있습니다.

정책 확인이 활성화되어 있지 않을 때 오류 있는 정책이 배포되는 경우 다른 명령의 오류에도 불구하고 일부 정책 명령이 여전히 실행될 수 있습니다.

정책 확인은 CA Access Control 데이터베이스 명령(AC 환경의 selang 명령)만 검사합니다. 정책 확인은 네이티브, 구성, 정책 모델 환경에서 명령을 검사하지 않습니다. 정책에 AC 환경의 명령과 다른 환경의 명령이 모두 포함되어 있으면 정책 확인은 AC 환경의 명령만 검사합니다.

정책 확인은 배포 취소 스크립트를 검사할 수 없습니다.

정책 확인이 작동하는 방법

정책 확인 기능은 끝점에 실제로 정책을 배포하기 전에 오류가 없는지 확인합니다.

참고: 정책 확인 기능은 기본적으로 활성화되어 있지 않습니다.

다음 절차는 정책 확인이 작동하는 방법에 대해 설명합니다.

1. 호스트 또는 호스트 그룹에 정책을 할당합니다.
2. 각 끝점에서 CA Access Control 엔터프라이즈 관리는 정책을 확인합니다.
3. 다음 중 하나가 발생합니다.
   - 정책에 오류가 없으면 CA Access Control 엔터프라이즈 관리가 정책을 끝점에 배포합니다.

     끝점이 정책 상태가 배포됨인 DMS 를 업데이트합니다.
   - 정책 스크립트에 오류가 있으면 CA Access Control 엔터프라이즈 관리는 정책을 끝점에 배포하지 않습니다.

     끝점이 정책 상태가 실행되지 않음인 DMS 를 업데이트합니다. DMS 는 또한 스크립트 오류가 있는 정책에 해당하는 각 배포 작업의 상태를 실패로 업데이트합니다.

     참고: CA Access Control 엔터프라이즈 관리의 배포 감사 기능을 사용하여 오류가 있는 스크립트를 볼 수 있습니다.

정책 확인 활성화

정책 확인 기능은 끝점에 실제로 정책을 배포하기 전에 오류가 없는지 확인합니다.

정책 확인 기능을 활성화하려면 policyfetcher 섹션의 policy_verification 구성 설정의 값을 1 로 설정하십시오.

그러면 정책 확인 기능이 활성화됩니다.

정책 버전 생성 및 저장

만들어 DMS 에 저장하는 모든 정책에는 자동으로 버전 번호가 지정됩니다. 처음 정책을 저장하면 버전 번호 "01"이 지정됩니다. 예를 들어 정책 myPolicy 를 처음 저장할 때 CA Access Control 엔터프라이즈 관리는 myPolicy 라는 GPOLICY 개체와 myPolicy#01 이라는 POLICY 개체를 만듭니다. DMS 에 이미 있는 정책을 저장할 때마다 저장된 최신 정책 버전이 한 버전씩 증가하면서 새로운 정책 버전이 작성됩니다. 예를 들어 myPolicy 버전을 28 번째 저장할 때 CA Access Control 엔터프라이즈 관리는 myPolicy#28 이라는 POLICY 개체를 작성합니다.

참고: 이 절차에서는 CA Access Control 엔터프라이즈 관리를 사용하여 정책 버전을 만들고 저장하는 방법에 대해 설명합니다. 이 절차는 UNAB 로그인 및 구성 정책에는 적용되지 않습니다.

정책 버전을 만들어 저장하려면

1. (선택 사항) selang 배포 명령을 사용하여 새 스크립트 파일을 작성합니다.

   이러한 명령은 기업의 끝점에 배포할 정책을 구성하는 데 필요한 명령입니다.

   중요! 정책 배포에서는 사용자 암호를 설정하는 명령을 지원하지 않으므로 배포 스크립트 파일에 이러한 명령을 포함시키지 마십시오. 네이티브 selang 명령이 지원되지만 위반 보고서에는 표시되지 않습니다.

2. (선택 사항) selang 배포 취소 명령을 사용하여 새 스크립트 파일을 작성합니다.

   이러한 명령은 기업의 끝점에서 정책을 배포 취소(제거)하는 데 필요한 명령입니다.

3. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 작업을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "정책" 트리를 확장합니다.

   정책 작업이 나타납니다.

4. "정책 만들기"를 클릭합니다.

   "정책 만들기: 정책 검색" 화면이 나타납니다.

   참고: 기존 정책에 대한 새 버전을 작성하려면 대신 "정책 수정"을 클릭하고 수정할 정책을 검색합니다.

5. "확인"을 클릭합니다.

   "정책 만들기" 작업 페이지가 나타납니다.

6. 대화 상자에서 다음 필드를 채웁니다.

   이름

   정책(GPOLICY 개체)의 이름을 정의합니다. 이 이름은 DMS 및 기업에서 고유해야 합니다. DMS 의 경우 이 사항이 강제 적용되며, 기업의 경우 강제 적용되지 않지만 동일한 이름의 정책이 이미 있으면 정책을 호스트에 배포할 수 없습니다.

   설명

   (선택 사항) 정책의 비즈니스 설명(자유 텍스트)을 정의합니다. 이 필드를 사용하여 이 정책이 나타내는 내용과 정책을 식별하는 데 도움을 주는 기타 정보를 기록하십시오.

7. "정책 스크립트" 탭을 클릭하고 다음 방법 중 하나를 사용하여 배포 및 배포 취소 스크립트를 제공합니다.

   - 배포 및 배포 취소 스크립트를 해당 필드에 입력합니다.

     배포 명령을 포함하는 스크립트 파일을 만들지 않았으면 이 옵션을 사용하십시오.

   - 기존 selang 스크립트 파일에서 명령을 로드합니다.

     a. "찾아보기"를 클릭하고 사용할 selang 스크립트가 포함된 파일을 찾습니다.

     b. "로드"를 클릭하여 스크립트 필드를 선택한 파일의 내용으로 채웁니다.

8. (선택 사항) 이 정책 버전에 대한 설명을 제공합니다.

   이 옵션을 사용하여 이 정책 버전에 사용할 배포 스크립트에 대한 특정 정보를 제공합니다.

9. (선택 사항) "제출 시 완료"를 선택합니다.

   이 옵션은 작성한 새 정책을 배포할 수 있도록 지정합니다. 배포 스크립트 작성을 완료하지 않은 경우에는 이 옵션의 선택을 취소합니다.

   참고: 이 옵션을 선택하지 않으면 새 정책 버전을 작성하지 않고 배포 스크립트를 수정할 수 있습니다. 그러나 완료되지 않은 정책 버전은 배포할 수 없습니다.

10. "정책 종속성" 탭을 클릭한 다음 "추가"를 클릭합니다.

    "구성원 추가" 대화 상자가 나타납니다.

11. 정책에 필수 구성 요소로 추가할 정책을 선택한 다음 "선택"을 클릭합니다.

    "구성원 추가" 대화 상자가 닫히고 선택한 정책이 정의 중인 정책의 "구성원 목록"에 추가됩니다.

12. "제출"을 클릭합니다.

    작업이 성공적으로 제출되면 새 정책 버전이 만들어졌음을 알리는 메시지가 바로 나타납니다.

참고: 또한 policydeploy 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. policydeploy 유틸리티에 대한 자세한 내용은 참조 안내서를 참조하십시오.

추가 정보:

UNAB 로그인 권한 부여 관리(페이지 139)
UNAB 호스트 또는 호스트 그룹 구성(페이지 141)

변수를 정의하는 정책 만들기

변수를 정의하는 정책을 만들어 배포하면 동일한 변수를 여러 끝점에서 정의할 수 있습니다.

변수를 정의하는 정책을 만들려면

1. 변수를 정의하는 selang 배포 명령을 사용하여 스크립트 파일을 만듭니다. 다음 selang 명령을 사용하여 각 변수를 정의합니다.

   ```
   editres ACVAR ("variable_name") value("variable_value")
   ```

2. (선택 사항) 변수를 사용하는 selang 명령을 스크립트 파일에 추가합니다.

   참고: 정책의 이후 규칙에서 변수를 참조하려면 정책의 각 변수를 정의해야 합니다. 변수를 참조할 때는 다음 형식을 사용하십시오: "<!variable>"

3. 정책을 DMS 에 저장합니다.

예: 변수를 정의하는 정책 만들기

이 예에서 다음 정책은 값이 /opt/jboss 이고 이름이 jboss_home 인 변수를 정의하고, 사용자 Mark 가 JBoss 를 통해 액세스하는 /opt 디렉터리에 있는 모든 리소스에 액세스하도록 허용하는 규칙을 만듭니다.

```
editres ACVAR ("jboss_home") value("/opt/jboss")
authorize FILE /opt/* uid(Mark) access(all) via(pgm("<!jboss_home>/jboss"))
```

끝점이 정책을 컴파일할 때 다음과 같은 규칙을 만듭니다.

```
authorize FILE /opt/* uid(Mark) access(all) via(pgm(/opt/jboss/jboss))
```

예: 여러 변수 값을 정의하는 정책 만들기

다음 정책은 다음과 같이 값이 C:\JBoss 이고 이름이 jboss_home 인 변수를 정의하고, C:\Program Files\JBoss 값을 jboss_home 변수에 추가하고, 액세스 규칙을 만듭니다.

```
editres ACVAR ("jboss_home") value("C:\JBoss")
editres ACVAR ("jboss_home") value+("C:\Program Files\JBoss")
editres FILE ("<!jboss_home>\bin") defacc(none) audit(a)
```

끝점이 정책을 컴파일할 때 다음과 같은 규칙을 만듭니다.

```
editres FILE ("C:\JBoss\bin") defacc(none) audit(a)
editres FILE ("C:\Program Files\bin") defacc(none) audit(a)
```

예: 변수를 사용하여 동일한 정책을 Windows 및 UNIX 끝점에 배포

다음 예는 운영 체제에서 JBoss 설치 위치가 다른 경우에도 변수를 사용하여 동일한 JBoss 정책을 Windows 및 UNIX 끝점에 배포하는 방법을 설명합니다. 이 예는 각 운영 체제에서 JBoss 설치 위치를 정의하는 두 개의 jboss_home 변수를 정의합니다.

1. 각 운영 체제의 JBoss 설치 위치를 정의하는 두 개의 jboss_home 변수를 정의합니다.
   - Windows 에서 JBoss 설치 위치를 정의하는 정책을 만들어 Windows 끝점에 배포합니다.

     ```
     editres ACVAR ("jboss_home") value("C:\JBoss")
     ```
   - UNIX 에서 JBoss 설치 위치를 정의하는 정책을 만들어 UNIX 끝점에 배포합니다.

     ```
     editres ACVAR ("jboss_home") value("/opt/jboss")
     ```
2. JBoss 설치 위치를 보호하기 위해 jboss_home 변수를 사용하는 정책을 만들어 Windows 및 UNIX 끝점에 배포합니다.

   ```
   editres FILE "<!jboss_home>" defacc(none) audit(all)
   ```
   - Windows 끝점이 이 정책을 컴파일할 때 다음 규칙을 만듭니다.

     ```
     editres FILE "C:\JBoss" defacc(none) audit(all)
     ```
   - UNIX 끝점이 이 정책을 컴파일할 때 다음 규칙을 만듭니다.

     ```
     editres FILE "/opt/jboss" defacc(none) audit(all)
     ```

정책과 연관된 규칙 보기

DMS 에 정책이 저장되면 각 정책 버전에 대한 배포 및 배포 취소 스크립트에서 규칙을 볼 수 있습니다.

정책과 연관된 규칙을 보려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "정책" 트리를 확장합니다.

   정책 작업이 나타납니다.
2. "정책 보기"를 클릭합니다.

   "정책 보기: 정책 검색" 화면이 나타납니다.
3. 검색 범위를 정의하고 "검색"을 클릭합니다.

   정의한 검색 범위와 일치하는 정책 목록이 나타납니다.

4. 볼 정책을 선택하고 "선택"을 클릭합니다.

   "정책 보기: policyName" 페이지가 나타납니다. 다양한 탭에서 정책 이름 및 설명, 최신 버전의 배포 및 배포 취소 스크립트, 이 정책에 대해 존재하는 모든 정책 버전 목록, 모든 정책 종속성, 정책 작성 및 업데이트 이벤트에 대한 일반적인 정보를 비롯한 정책 속성을 볼 수 있습니다.

5. 버전 기록 탭을 누릅니다.

   정책 버전 목록이 나타나고 각 버전에는 배포 및 배포 취소 스크립트 링크가 포함되어 있습니다.

6. 다음 중 하나를 수행합니다.

   - "배포 스크립트" 링크를 클릭합니다.

     배포 스크립트가 포함된 팝업 창이 나타납니다.

   - "배포 취소 스크립트" 링크를 클릭합니다.

     배포 취소 스크립트가 포함된 팝업 창이 나타납니다.

참고: 또한 policydeploy 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. policydeploy 유틸리티에 대한 자세한 내용은 참조 안내서를 참조하십시오.

정책 가져오기

정책을 가져올 때 CA Access Control 엔터프라이즈 관리는 로컬 CA Access Control 데이터베이스 또는 PMDB 에서 selang 규칙을 내보내 DMS 에 이 규칙을 포함하는 정책을 만들어 저장합니다. 이렇게 하면 한 끝점을 보호하는 규칙을 여러 끝점을 보호할 수 있는 정책으로 변환할 수 있으므로 PMDB 를 고급 정책 관리로 마이그레이션하는 데 도움이 됩니다.

참고: 규칙을 내보내는 끝점 또는 PMDB 는 CA Access Control r12.0 이상이 설치된 호스트에 있어야 합니다. 이전 CA Access Control 버전에서 정책을 가져오려면 우선 끝점을 업그레이드하십시오.

정책을 가져오려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.

   a. "정책 관리"를 클릭합니다.

   b. "정책" 하위 탭을 클릭합니다.

   c. 작업 메뉴에서 왼쪽에 있는 "정책" 트리를 확장합니다.

      사용 가능한 작업 목록에 "정책 가져오기" 작업이 나타납니다.

2. "정책 가져오기"를 클릭합니다.

   "호스트 로그인" 페이지가 나타납니다.

3. 사용자 이름, 암호, 규칙을 내보낼 원본 PMDB 또는 호스트의 이름을 입력한 다음 "로그인"을 클릭합니다.

   참고: master_pmdb@example 과 같이 PMDBname@host 형식으로 PMDB 이름을 지정하십시오.

   "일반" 작업 단계에 "정책 가져오기 프로세스" 마법사가 나타납니다.

4. 다음 필드를 완성하고 "다음"을 클릭합니다.

   이름

   정책 이름을 정의합니다. 이 이름은 DMS 및 회사에서 고유해야 합니다(회사에서 반드시 고유한 이름을 사용할 필요는 없지만 동일한 이름의 정책이 이미 있으면 정책을 호스트에 배포할 수 없음).

   설명

   (선택 사항) 정책의 비즈니스 설명(자유 텍스트)을 정의합니다. 이 필드를 사용하여 이 정책이 나타내는 내용과 정책을 식별하는 데 도움을 주는 기타 정보를 기록하십시오.

   정책 클래스

   내보내 정책에 포함할 규칙이 있는 클래스를 지정합니다. 선택 목록 열에 클래스를 지정하지 않으면 모든 클래스를 내보내 정책에 포함합니다.

   종속된 클래스 내보내기

   선택 목록 열에 지정하는 클래스에 종속된 모든 클래스를 내보내도록 지정합니다. 이 옵션을 선택하지 않으면 CA Access Control 은 선택 목록 열에 지정하는 클래스만 내보냅니다.

   "정책 스크립트" 단계가 나타납니다.

5. 내보낸 규칙을 검토하고 필요한 경우 이 규칙을 수정한 후 "다음"을 클릭합니다.

   "요약" 단계가 나타납니다.

6. "마침"을 클릭합니다.

   정책이 만들어집니다.

저장된 정책 버전 할당

특정 호스트나 호스트 그룹에 여러 규칙 정책의 완료된 최신 버전을 할당할 수 있습니다. 할당된 정책은 자동으로 배포되며 DMS 에서 해당 상태를 모니터링할 수 있습니다.

참고: 이 절차는 로그인 및 구성 정책에는 적용되지 않습니다.

저장된 정책 버전을 할당하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "할당" 트리를 확장한 다음 "정책 할당"을 클릭합니다.

   정책 선택 작업 단계에서 "정책 할당" 마법사가 나타납니다.

2. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.

   CA Access Control 이 정책 할당 작업을 제출합니다. 정책이 호스트에 직접 할당되거나 논리 호스트 그룹 구성원을 통해 할당되면 CA Access Control 에서는 검색할 각 호스트에 대해 DEPLOYMENT 작업을 생성합니다.

참고: 또한 policydeploy 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. policydeploy 유틸리티에 대한 자세한 내용은 참조 안내서를 참조하십시오.

정책 유지 관리

배포된 정책에 대해 다음 작업을 수행할 수 있습니다.

- 할당된 호스트에서 정책 할당 취소
- 호스트를 최신 정책 버전으로 업그레이드
- 호스트를 이전 정책 버전으로 다운그레이드
- 배포된 정책의 오류 검사
- 정책 또는 정책 버전 삭제

이러한 작업은 CA Access Control 엔터프라이즈 관리에서 수행하거나 policydeploy 유틸리티를 사용하여 수행합니다.

할당된 정책 할당 취소

특정 호스트에서 또는 호스트 그룹으로 할당된 정책을 할당 취소할 수 있습니다. 할당 취소된 정책은 자동으로 배포 취소됩니다.

할당된 정책을 할당 취소하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "할당" 트리를 확장한 다음 "정책 할당 취소"를 클릭합니다.

   정책 선택 작업 단계에서 "정책 할당 취소" 마법사가 나타납니다.

2. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.

   CA Access Control 이 정책 할당 작업을 제출합니다. 정책이 호스트에서 직접 할당 취소되거나 논리 호스트 그룹 구성원을 통해 할당 취소되면 CA Access Control 에서는 검색할 각 호스트에 대해 DEPLOYMENT 작업을 생성합니다.

참고: 또한 policydeploy 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. policydeploy 유틸리티에 대한 자세한 내용은 참조 안내서를 참조하십시오.

할당된 호스트를 최신 정책 버전으로 업그레이드

새 정책 버전은 할당된 호스트나 정책이 배포된 호스트로 자동으로 전송되지 않습니다. 정책이 배포된 호스트를 최신 정책 버전으로 수동으로 업그레이드해야 합니다.

할당된 호스트를 최신 정책 버전으로 업그레이드하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "할당" 트리를 확장한 다음 "정책 업그레이드"를 클릭합니다.

   정책 선택 작업 단계에서 "정책 업그레이드" 마법사가 나타납니다.

2. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.

   CA Access Control 이 정책 업그레이드 작업을 제출합니다. 호스트의 정책을 업그레이드하기 위해 CA Access Control 에서는 검색할 호스트에 대해 DEPLOYMENT 작업을 생성합니다.

   참고: 업그레이드할 호스트 그룹을 선택할 때 CA Access Control 엔터프라이즈 관리는 배포된 정책의 오래된 버전이 있는 호스트를 수록한 호스트 그룹에서만 선택할 수 있게 합니다.

참고: 또한 policydeploy 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. policydeploy 유틸리티에 대한 자세한 내용은 참조 안내서를 참조하십시오.

할당된 호스트를 특정 정책 버전으로 다운그레이드

잘못된 정책 버전을 하나 이상의 호스트에 실수로 할당했거나 특정 호스트에서 이전 정책 버전으로 돌아가려는 경우 정책을 다운그레이드할 수 있습니다.

할당된 호스트를 특정 정책 버전으로 다운그레이드하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "할당" 트리를 확장한 다음 "정책 다운그레이드"를 클릭합니다.

   정책 선택 작업 단계에서 "정책 다운그레이드" 마법사가 나타납니다.

2. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.

   CA Access Control 이 정책 다운그레이드 작업을 제출합니다. 호스트의 정책을 다운그레이드하기 위해 CA Access Control 에서는 검색할 호스트에 대해 DEPLOYMENT 작업을 생성합니다.

참고: 또한 policydeploy 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. policydeploy 유틸리티에 대한 자세한 내용은 참조 안내서를 참조하십시오.

삭제된 정책

논리 정책(GPOLICY 개체) 또는 정책 버전(POLICY 개체)을 DMS 에서 삭제할 수 있습니다. 정책 버전을 삭제할 때 CA Access Control 엔터프라이즈 관리는 또한 해당 정책 버전과 관련된 배포 및 배포 취소 스크립트(RULESET 개체)도 삭제합니다. 논리 정책을 삭제하면 논리 정책과 관련된 모든 정책 버전 및 관련 스크립트도 삭제됩니다.

삭제된 논리 정책 또는 정책 버전은 복원할 수 없습니다.

삭제할 수 없는 정책

다음과 같은 경우 정책을 삭제할 수 없습니다.

- 하나 이상의 정책의 정책 버전을 삭제할 수 없는 경우
- 정책이 다른 정책의 필수 구성 요소인 경우

  정책을 삭제하기 전에 정책의 모든 종속성을 제거해야 합니다.
- 정책이 호스트에 할당 또는 배포된 경우

  정책을 삭제하기 전에 호스트에서 정책을 할당 취소 또는 배포 취소해야 합니다.

삭제할 수 없는 정책 버전

다음과 같은 경우 정책 버전을 삭제할 수 없습니다.

- 정책 버전이 호스트에 할당 또는 배포된 경우

  정책 버전을 삭제하기 전에 호스트에서 정책 버전을 할당 취소 또는 배포 취소해야 합니다.

- 정책 버전이 DMS 에서 상태가 있는 경우

  정책 버전을 삭제하기 전에 정책 버전을 할당 취소 또는 배포 취소하거나 호스트에서 정책 버전을 제거해야 합니다.

- 정책의 상태가 "배포 취소되었지만 오류 발생"인 경우

  이 상태는 제거할 수 없습니다. 정책 버전은 삭제할 수 없습니다.

정책 삭제

정책이 호스트 또는 호스트 그룹에 더 이상 할당되어 있지 않은 경우 CA Access Control 엔터프라이즈 관리에서 이 정책을 삭제할 수 있습니다.

중요! 정책(GPOLICY 개체)을 삭제할 때 CA Access Control 엔터프라이즈 관리는 모든 정책 버전(POLICY 개체)과 각 정책 버전과 연계된 RULESET 개체를 삭제합니다.

정책을 삭제하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "정책" 트리를 확장합니다.

   정책 작업이 나타납니다.

2. "정책 삭제"를 클릭합니다.

   "정책 삭제: 정책 검색" 화면이 나타납니다.

3. 검색 범위를 정의하고 "검색"을 클릭합니다.

   정의한 검색 범위와 일치하는 정책 목록이 나타납니다.

4. 삭제할 정책을 선택하고 "선택"을 클릭합니다.

   정책을 삭제할지 묻는 메시지가 표시됩니다.

5. "예"를 클릭합니다.

   정책이 삭제됩니다.

참고: 또한 policydeploy 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. policydeploy 유틸리티에 대한 자세한 내용은 참조 안내서를 참조하십시오.

추가 정보:

삭제할 수 없는 정책(페이지 78)

정책 버전 삭제

더 이상 필요 없는 저장된 정책 버전(POLICY 개체)을 삭제할 수 있습니다. 정책 버전(POLICY 개체)을 삭제할 때 CA Access Control 엔터프라이즈 관리는 이 정책 버전과 연계된 모든 배포 및 배포 취소 스크립트를 삭제합니다.

정책 버전을 삭제하려면 다음 명령을 실행하십시오.

```
policydeploy -delete name#xx [-dms list]
```

-delete name#xx

지정된 정책 버전을 삭제합니다.

-dms list

(선택 사항) 정책 버전을 삭제할 DMS 노드의 쉼표로 구분된 목록을 지정합니다. DMS 노드를 지정하지 않으면 policydeploy 유틸리티는 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록을 사용합니다.

예: IIS 5 보호 정책 버전 삭제

다음 예는 할당 취소된 정책 버전 IIS5#05 를 DMS 에서 삭제하는 방법에 대해 설명합니다. 이 예에서 정책 버전 IIS5#05 는 어떠한 호스트 또는 호스트 그룹에도 할당되지 않았으며 crDMS@cr_host.company.com DMS 노드에 저장되어 있습니다.

IIS 5 보호 정책 버전을 삭제하려면 명령 프롬프트 창을 연 다음 policydeploy 유틸리티를 실행하십시오.

```
policydeploy -delete IIS5#05
```

정책 버전 IIS5#05 가 crDMS@cr_host.company.com DMS 노드에서 삭제됩니다.

변수

변수는 다른 구성 및 운영 체제를 사용하는 끝점에 동일한 정책을 배포할 수 있게 해 줍니다. 예를 들어, 변수를 사용하여 운영 체제의 다른 위치에 CA Access Control 이 설치되어 있는 경우라도 동일한 정책을 Windows 및 Solaris 끝점에 배포할 수 있습니다.

변수 작성 방법

변수는 ACVAR 클래스의 개체이고 하나 이상의 값을 가질 수 있습니다. 끝점에 있는 각 변수와 정책의 각 변수에는 고유한 이름을 사용해야 합니다. 다음 중 한 방법으로 변수를 만들 수 있습니다.

- CA Access Control 끝점 관리를 사용하여 끝점에서 변수를 정의합니다.
- 변수를 정의하는 정책을 만들어 여러 끝점에 배포합니다.

중요! 정책의 변수를 사용하는 규칙만 만들 수 있습니다. 변수를 포함하는 규칙을 사용하여 CA Access Control 데이터베이스를 직접 업데이트하면 데이터베이스가 규칙을 컴파일할 수 없고 CA Access Control 이 이 규칙을 시행할 수 없습니다. 정책 스크립트에서 변수를 참조하기 전에 변수를 정의해야 합니다.

변수 유형

CA Access Control 은 사용자 정의된 변수 및 기본 제공되는 변수를 지원합니다.

- 사용자 정의된 변수는 CA Access Control 데이터베이스에 정의하는 변수입니다.
- 기본 제공되는 변수는 CA Access Control 이 설치 중 생성하는 변수입니다. 기본 제공되는 변수는 수정할 수 없습니다.

사용자 정의된 변수

CA Access Control 은 다음과 같은 사용자 정의된 변수를 지원합니다.

정적 변수

CA Access Control 끝점의 고정된 위치를 정의합니다.

이름이 같지만 값이 다른 정적 변수를 여러 개 정의할 수 있지만 각 변수는 반드시 다른 끝점 및 다른 정책에 존재해야 합니다.

참고: 변수를 만들 때 변수 유형을 지정하지 않으면 CA Access Control 은 정적 변수를 만듭니다.

레지스트리 값 변수

(Windows) 레지스트리 값을 기반으로 CA Access Control 끝점의 위치를 정의합니다.

참고: REG_SZ 또는 REG_EXPAND_SZ 레지스트리 유형을 가리키는 레지스트리 변수만 정의할 수 있습니다.

예: 다음 규칙은 이름이 jboss_home 인 레지스트리 변수를 정의합니다.

```
editres ACVAR ("jboss_home") value("HKLM\Software\Jboss\home") type(regval)
```

정책에 이 규칙을 배포할 때 Windows 끝점은 HKLM\Software\Jboss\home 레지스트리 키를 사용하여 변수 값을 가져옵니다.

운영 체제 변수

운영 체제 환경 값을 기반으로 CA Access Control 끝점의 위치를 정의합니다.

예: 다음 규칙은 이름이 jboss_home 인 운영 체제 변수를 정의합니다.

```
editres ACVAR (“jboss_home”) value(“JBOSS_HOME”) type(osvar)
```

정책에 이 규칙을 배포할 때 끝점은 JBOSS_HOME 운영 체제 환경 변수의 값을 사용하여 변수 값을 가져옵니다.

기본 제공되는 변수

CA Access Control 은 설치 프로세스 중 CA Access Control 데이터베이스에 기본 제공되는 변수를 만듭니다. 기본 제공되는 변수를 수정하거나 삭제할 수 없지만 기본 제공되는 변수를 정책에 사용할 수 있습니다. 기본 제공되는 변수는 동적 변수이며 CA Access Control 끝점의 시스템 설정에 종속됩니다. 기본 제공되는 변수의 값은 해당 시스템 설정이 변경될 때 함께 변경됩니다.

참고: CA Access Control 데이터베이스를 내보낼 때 기본 제공되는 변수는 출력에 포함되지 않습니다. CA Access Control 은 DMS 또는 PMDB 를 만들 때 기본 제공되는 변수를 만들지 않습니다.

CA Access Control 은 다음과 같은 기본 제공되는 변수를 지원합니다.

<!HOSTNAME>

로컬 컴퓨터의 정규화된 호스트 이름을 식별합니다.

<!HOSTIP>

하나 이상의 호스트 IP 주소를 식별합니다.

<!AC_ROOT_PATH>

CA Access Control 설치 경로를 식별합니다.

<!AC_REGISTRY_KEY>

(Windows) CA Access Control 루트 레지스트리 키를 식별합니다.

<!USER_OS_ADMIN>

로컬 컴퓨터 운영 체제의 관리자를 식별합니다.

<!DOMAINNAME>

로컬 컴퓨터의 도메인 이름을 식별합니다.

<!DNSDOMAINNAME>

로컬 컴퓨터의 DNS 이름을 식별합니다.

예: 정책에 기본 제공되는 변수 사용

이 예는 다음과 같이 네트워크 리소스 규칙을 만듭니다.

```
authorize TCP 8333 uid(*) host(<!HOSTNAME>) access(WRITE)
```

이 정책을 끝점 host1.example.com 과 이 정책을 준수하는 끝점에 배포하면 다음 규칙이 만들어집니다.

```
authorize TCP 8333 uid(*) host(host1.example.com) access(WRITE)
```

변수 사용 지침

변수를 사용할 때 다음과 같은 지침을 따라야 합니다.

- 다른 변수나 정책이 사용하는 변수는 삭제할 수 없습니다.
- 변수는 여러 값을 가질 수 있습니다. 변수 값을 추가 또는 제거할 수 있습니다.
- 변수는 중첩될 수 있습니다. 예를 들어, 다음 규칙은 기본 제공되는 <!AC_ROOT_PATH> 변수를 포함하는 ac_data 란 이름의 변수를 정의합니다.

  ```
  editres ACVAR ac_data value("<!AC_ROOT_PATH>\data")
  ```

  기본 설치된 CA Access Control 이 있는 Windows 끝점이 이 규칙을 준수하면 다음 규칙이 만들어집니다.

  ```
  editres ACVAR ac_data value("C:\Program Files\CA\AccessControl\data")
  ```

- 각 변수는 하나의 유형만 가질 수 있으므로, 예를 들어 변수를 정적 변수인 동시에 레지스트리 값 변수로 정의할 수 없습니다.
- 정의되지 않은 변수를 포함하는 정책을 배포할 수 없습니다. 정의되지 않은 변수를 포함하는 정책을 배포하면 CA Access Control 이 이 정책의 배포 상태를 "배포 보류"로 변경합니다. 정책을 배포하려면 우선 정의되지 않은 변수를 정의한 다음 정책을 다시 배포해야 합니다.

  참고: 정책에서 정의되지 않은 변수를 찾으려면 정책의 DEPLOYMENT 개체를 검토하십시오. CA Access Control 은 정책 검사의 활성화 여부에 관계없이 정의되지 않은 변수를 검사합니다.

- CA Access Control 은 CA Access Control 변수와 Windows 시스템 변수를 결합하는 규칙을 해석할 수 없습니다. 예를 들어, CA Access Control 은 이름이 var1 인 변수를 정의하는 다음 규칙을 해석할 수 없습니다.

  ```
  editres ACVAR var1 value("%SYSTEMROOT%\temp")
  ```

  %SYSTEMROOT%를 CA Access Control 변수로 정의하고 %SYSTEMROOT%\temp 를 보호하는 정책을 만들려면 다음 규칙을 사용하십시오.

  ```
  editres ACVAR var1 value("SYSTEMROOT") type(osvar)
  editres ACVAR var2 value("<!var1>\temp")
  ```

- CA Access Control 은 서로 종속된 변수를 확인할 수 없습니다. 예를 들어, CA Access Control 은 다음 예에서 변수 var1 과 var2 를 해석할 수 없습니다.

  ```
  editres ACVAR var1 value("<!var2>")
  editres ACVAR var2 value("<!var1>")
  ```

- 슬래시를 사용하여 변수에서 디렉터리를 정의할 때 CA Access Control 은 Windows 와 UNIX 끝점에 대해 슬래시를 올바른 방향으로 해석합니다.
- selang 규칙을 사용하여 변수를 정의하는 경우 정책을 사용하여 규칙을 끝점에 배포해야 합니다. selang 규칙을 사용하여 끝점에 있는 CA Access Control 데이터베이스를 직접 업데이트하면 CA Access Control 은 이 규칙을 컴파일할 수 없습니다. 예를 들어, 끝점에서 jboss_home 이란 이름의 변수를 정의하고 다음 selang 규칙으로 데이터베이스를 직접 업데이트했다고 가정합니다.

  ```
  editres FILE <!jboss_home> audit(all)
  ```

  CA Access Control 은 이 규칙을 컴파일할 수 없지만 대신 데이터베이스에 <!jboss_home>이란 이름의 FILE 개체를 만듭니다.

끝점이 변수를 해석하는 방법

변수는 다른 구성 및 운영 체제를 사용하는 끝점에 동일한 정책을 배포할 수 있게 해 줍니다. 다음 프로세스는 정책을 만들어 배포한 이후에 CA Access Control 끝점이 정책에 있는 변수를 해석하는 방법을 설명합니다.

1. policyfetcher 가 정책을 가져오면 CA Access Control 은 이 정책에 있는 변수가 정책 또는 CA Access Control 데이터베이스에 정의되어 있는지 확인합니다. 다음 중 하나가 발생합니다.
   - 변수가 정책 또는 데이터베이스에 정의되어 있지 않으면 CA Access Control 이 정책 상태를 "배포 보류"로 변경합니다.

     참고: 정책을 배포하려면 우선 정의되지 않은 변수를 정의한 다음 정책을 다시 배포해야 합니다.
   - 변수가 정책 또는 데이터베이스에 정의되어 있으면 CA Access Control 은 이 정책을 컴파일하고 포함된 규칙을 시행합니다.
2. 하트비트때마다 policyfetcher 는 CA Access Control 데이터베이스에서 변수 값이 변경되었는지 확인합니다.다음 중 하나가 발생합니다.
   - 변수 값이 변경되지 않았으면 policyfetcher 는 2 단계를 반복합니다.
   - 변수 값이 변경되었으면 CA Access Control 은 변경된 변수를 사용하는 끝점에 있는 모든 정책에 대해 정책 상태를 "동기화되지 않음"으로 변경합니다.

     참고: 정책에 대한 "동기화되지 않음" 상태를 지우려면 정책을 다시 배포해야 합니다.

정책 배포 문제 해결

호스트에 정책을 할당할 때 policyfetcher 가 배포 작업을 검색하고 정책 스크립트를 실행할 때까지 정책은 할당된 끝점에 배포되지 않습니다. 따라서 정책이 전송되거나 끝점에 배포될 때 다양한 이유로 배포 오류가 발생할 수 있습니다.

정책 배포 오류를 해결하기 위해 고급 정책 관리에는 문제 해결 작업을 제공합니다. 이러한 작업은 CA Access Control 엔터프라이즈 관리 또는 policydeploy 유틸리티를 사용하여 수행할 수 있습니다. CA Access Control 엔터프라이즈 관리에서 문제 해결 작업은 "정책 관리" 탭의 "정책" 하위 탭에 있습니다.

문제 해결 작업은 다음과 같습니다.

- **재배포** - 정책 스크립트를 포함하는 새 배포 작업을 만들어 끝점에 배포합니다.

  정책을 끝점에 배포할 때 오류가 발생하는 경우 이 옵션을 사용하십시오. 즉, selang 정책 스크립트 실행이 실패하는 경우입니다. 정책을 재배포하려면 먼저 끝점에서 스크립트 오류의 원인을 수동으로 수정해야 합니다.

  참고: 이 옵션은 CA Access Control 엔터프라이즈 관리에서만 사용할 수 있으며 policydeploy 유틸리티에서는 지원되지 않습니다.

- **배포 취소** - 해당 호스트에서 정책을 할당 취소하지 않고 지정된 끝점에서 정책의 배포를 취소합니다.

  DMS 에 있는 호스트에 할당되지 않은 끝점에서 정책을 제거하려면 이 옵션을 사용하십시오.

- **다시 설정** - 끝점을 다시 설정합니다. CA Access Control 은 호스트 상태를 재설정하고, 모든 유효 정책을 배포 취소하며, 모든 고급 정책 관리 개체를 삭제합니다.

  배포와 고급 정책 관리 속성에서 DMS 의 끝점 및 해당 상태를 정리하려면 이 옵션을 사용하십시오.

- **복원** - 지정된 호스트에서 모든 정책의 배포를 취소한 다음, 모든 배포 작업을 실행을 위해 호스트로 다시 전달함으로써 호스트에 배포해야 할 모든 정책을 복원(직접 재배포)합니다.

  DMS 에서 한 끝점에 대해 유효하다고 표시하는 모든 정책을 재배포하기 위해 해당 끝점을 수동으로 재설정(CA Access Control 또는 운영 체제 재설치)하려면 이 옵션을 사용하십시오.

  참고: 호스트에 이미 몇몇 정책이 적용되었으면 실행 전에 호스트 상태가 재설정되지 않으므로 복원이 실패합니다.

사용하지 않는 끝점 제거 방법

DMS 에서는 기업에 대한 정보를 저장합니다. 기업에서 컴퓨터를 제거하는 경우 이 컴퓨터에서 CA Access Control 을 제거해도 DMS 에는 해당 노드에 대한 참조가 계속 포함되어 있습니다. 일상적인 유지 관리 절차로서 DMS 에서 이런 사용하지 않는 노드를 정리해야 합니다.

사용하지 않는 노드를 제거하려면 다음 중 하나를 수행하십시오.

- DMS 컴퓨터에서 다음과 같이 dmsmgr 유틸리티를 실행하여 일상적인 정리 작업을 수행합니다.

  ```
  dmsmgr -cleanup number_of_days -dms name
  ```

  number_of_days

  CA Access Control 노드를 사용할 수 없는 최소 일 수를 정의합니다.

- DMS 컴퓨터에서 다음 selang 명령을 실행하여 특정 노드를 수동으로 삭제합니다.

  ```
  rr HNODE HNODE_name
  ```

중요! 노드를 삭제하면 CA Access Control 에서는 모든 HNODE 관련 배포 작업을 제거하고, 패키지에 다른 배포 작업 구성원이 포함되지 않은 한 모든 배포 작업의 패키지를 제거한 다음, HNODE 개체만 제거합니다.

배포 감사 정보 보기

CA Access Control 엔터프라이즈 관리에서는 정책 배포 감사 기능을 제공합니다. 이 감사는 배포 작업의 설명 목록인 정책 배포 보기를 제공합니다. 이 목록에는 각 배포 작업을 트리거한 항목, 작업이 생성된 시간 및 관련된 배포 유형이 자세히 설명되어 있습니다. 각 배포 작업에 대해 배포 작업이 생성된 호스트 및 정책 쌍, 배포된 정책 버전, 배포 작업 상태(큐에 추가, 성공 또는 실패) 및 selang 출력(명령 배포 결과) 등의 세부 정보를 추가로 탐색할 수 있습니다.

배포 감사 정보를 보려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "정책 관리"를 클릭합니다.
   b. "정책" 하위 탭을 클릭합니다.
   c. 작업 메뉴에서 왼쪽에 있는 "배포" 트리를 확장합니다.

      사용 가능한 작업 목록에 "배포 감사" 작업이 나타납니다.
2. "배포 감사"를 클릭합니다.

   "배포 감사" 페이지가 나타납니다.
3. 배포 감사 범위를 정의하고 "실행"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 정의된 범위 내에 있는 배포 정보를 검색하고 잠시 후 결과를 표시합니다.
4. (선택 사항) 연관된 배포 작업에 대한 자세한 내용을 보려면 배포의 트리거를 클릭합니다.

정책 위반 계산 작동 방법

고급 정책 관리를 사용하면 정책 배포의 결과로 끝점에 배포되어야 하는 액세스 규칙과 동일한 끝점에 성공적으로 배포된 실제 규칙 사이의 차이점을 확인할 수 있습니다. 또한 정책 개체에 추가된 속성과 변경된 속성을 확인합니다. 이 정보를 사용하면 정책 배포와 연관된 문제를 해결할 수 있습니다.

끝점에서 정책 위반 계산기를 실행하면 다음 작업이 수행됩니다.

1. 끝점에 배포해야 하는 규칙 목록을 로컬 호스트에서 검색합니다.

   이러한 규칙은 배포된 각 정책 버전의 POLICY 개체와 연관된 로컬 RULESET 개체에 지정된 대로 각 배포 정책에 지정된 규칙입니다.

2. 이러한 각 규칙이 끝점에 적용되는지 확인합니다.

   중요! 위반 계산에서는 기본 규칙이 적용되는지 여부를 확인하지 않습니다. 또한 데이터베이스에서 개체(사용자 또는 개체 특성, 사용자 또는 리소스 권한 부여, 실제 사용자 또는 리소스)를 제거하는 규칙을 무시합니다. 예를 들어 위반 계산에서는 다음 규칙이 적용되는지 여부를 확인할 수 없습니다.
   rr FILE /etc/passwd

3. (선택 사항) 로컬 정책 개체와 DMS 의 정책 개체를 비교합니다.

   일반적으로 위반 계산기는 로컬 호스트에서만 위반을 확인합니다. -strict 옵션을 지정하면 위반 계산기가 로컬 HNODE 개체와 연관된 정책과 DMS 에 있는 HNODE 개체와 연관된 정책도 비교합니다. 비교하는 내용은 다음과 같습니다.

   a. 로컬 호스트를 나타내는 HNODE 개체와 연관된 정책 목록

   b. HNODE 개체와 연관된 각 POLICY 개체의 정책 상태

   c. HNODE 개체와 연관된 각 POLICY 개체의 정책 서명

4. 다음 두 개의 파일이 출력됩니다.

   - ACInstallDir/data/devcalc/deviation.log

     마지막 위반 계산 시 수집된 로그 및 오류 메시지입니다.

   - ACInstallDir/data/devcalc/deviation.dat

     정책 및 해당 위반 목록입니다. 끝점에서 selang 명령 get devcalc 를 사용하여 이 파일의 내용을 가져올 수 있습니다.

   참고: CA Access Control 은 seaudit -a 를 사용하여 볼 수 있는 감사 이벤트도 전송합니다. seaudit 유틸리티에 대한 자세한 내용은 참조 안내서를 참조하십시오.

5. 위반이 있음을 DMS 에 알립니다.

알림은 로컬 CA Access Control 데이터베이스에 대해 지정된 DH 를 통해 DMS 에 전달됩니다.

위반 계산 트리거

DMS 에 정책 위반 상태에 대한 최신 정보가 포함되도록 위반 계산을 정기적으로 수행해야 합니다. 끝점에서 고급 정책 관리가 비활성화된 경우 policyfetcher 가 각 하트비트 이후에 위반 계산을 트리거합니다.

원하는 간격으로 정책 위반 계산이 수행되도록 policyfetcher 설정을 수정하는 것이 좋습니다.

정책 위반 로그 및 오류 파일

정책 위반을 계산하면 각 위반 계산 중에 새 로그가 작성됩니다. 오류 메시지도 포함되어 있는 이 로그는 ACInstallDir/data/devcalc/deviation.log 에 저장되어 있습니다.

DMS 에서 가져온 보고서에 표시되는 위반이 마지막으로 실행된 위반 계산에서 수집되지 않은 경우 이 로그를 사용합니다. 이 로그는 위반 계산 결과가 DMS 로 전송되지 않은 이유를 진단하는 데 도움이 됩니다.

예: 위반 로그 및 오류 파일

다음은 예제 위반 로그와 오류 파일입니다.

```
시작 시간: Mon Jan 23 13:04:48 2006
경고,\"DH 호스트 이름을 검색하지 못했습니다. 위반이 로컬에 저장됩니다.\"
'iis8#02' 정책에 대한 위반을 찾았습니다.
종료 시간: Mon Jan 23 13:05:04 2006
```

정책 위반 데이터 파일

정책 위반을 계산하면 정책 및 정책 위반 목록이 포함된 데이터 파일이 작성됩니다. 이 데이터 파일은 ACInstallDir/data/devcalc/deviation.dat 에 저장되어 있습니다.

참고: 데이터 파일에 포함되는 정책 목록은 위반을 계산하는 정책에 따라 다릅니다. 기본적으로 끝점의 모든 정책과 모든 정책 버전이 포함됩니다.

중요! 위반 계산에서는 네이티브 규칙이 적용되는지 여부를 확인하지 않습니다. 또한 데이터베이스에서 개체(사용자 또는 개체 특성, 사용자 또는 리소스 권한 부여, 실제 사용자 또는 리소스)를 제거하는 규칙을 무시합니다. 예를 들어 위반 계산에서는 다음 규칙이 적용되는지 여부를 확인할 수 없습니다.
rr FILE /etc/passwd

위반이 있는지 여부에 관계없이 위반 상태는 DMS 로 전송되지만 실제 위반은 로컬에 저장됩니다. 보고서 작성 시 이 파일에서 실제 위반 결과를 가져와서 보고서에 추가할 수 있습니다.

정책 위반 데이터 파일에 나타날 수 있는 줄은 다음과 같습니다.

Date

위반 계산의 타임스탬프를 표시합니다. 날짜 줄은 항상 위반 보고서의 첫 번째 줄입니다.

형식: DATE, DDD MMM DD hh:mm:ss YYYY

Strict

-strict 옵션을 사용하여 위반 계산이 실행되었음을 지정합니다.

형식: STRICT, DMS@hostname, policy_name#xx, [1|0]

[1|0]은 로컬 HNODE 개체와 연관된 정책과 DMS@hostname 의 HNODE 개체와 연관된 정책 사이에 위반이 있는지(1) 또는 없는지(0) 여부를 나타냅니다.

Policy Start

이 정책 버전에 대한 위반을 정의하는 정책 블록을 시작합니다.

형식: POLICYSTART, policy_name#xx

Difference

정책에 대해 발견된 위반을 설명합니다. 위반이 적용되는 정책 이름은 이 줄 위에서 가장 가까운 정책 줄입니다.

다음 표에는 누락 요소를 나타내는 위반 네 개 및 추가 요소를 나타내는 위반 네 개의 위반 유형 여덟 개가 설명되어 있습니다.

위반 유형	형식
클래스를 찾을 수 없습니다.	DIFF, -(class_name), (*), (*), (*)
개체를 찾을 수 없습니다.	DIFF, (class_name), -(object_name), (*), (*)
개체가 추가되었습니다.	DIFF, (class_name), +(object_name), (*), (*)
속성을 찾을 수 없습니다.	DIFF, (class_name), (object_name), -(property_name), (*)
속성이 추가되었습니다.	DIFF, (class_name), (object_name), +(property_name), (*)
속성 값이 없습니다.	DIFF, (class_name), (object_name), (property_name), -(expected_value)
속성 값이 추가되었습니다.	DIFF, (class_name), (object_name), (property_name), +(expected_value)

참고: 위반 계산기는 누락된 클래스를 발견하면 누락된 모든 개체, 속성 및 값에 대한 위반 줄을 생성합니다.

Policy End

이 정책에 대한 위반을 정의하는 정책 블록을 종료합니다.

형식: POLICYEND, policy_name#xx, [1|0]

{1|0}은 위반이 있는지(1) 또는 없는지(0) 여부를 나타냅니다.

Warning

경고를 설명합니다.

형식: WARNING, "warning_text"

예: 위반 데이터 파일

다음 예는 위반 데이터 파일의 내용을 보여 줍니다.

```
Date: Sun Mar 19 08:30:00 2006
WARNING, "DH 호스트 이름을 검색하지 못했습니다. 위반이 로컬에 저장됩니다"
POLICYSTART, iis8#02
DIFF, (USER), (iispers), (*), (*)
POLICYEND, iis8#02, 1
```

누락된 요소를 나타내는 위반

위반 계산기는 누락된 요소와 추가된 새 요소를 구별합니다. 누락된 요소는 지정된 정책에 명시적으로 정의되어 있지만 로컬 호스트에 없는 CA Access Control 요소입니다. 이러한 누락된 요소는 클래스, 개체, 속성 및 값이 될 수 있습니다.

누락된 요소 조합은 계층적 요구 사항을 정의합니다. 예를 들어 Policy1 에는 다음 규칙이 있습니다.

```
eu mytestuser2 operator
```

위반 계산기는 다음 암시적 요구 사항이 충족된다고 가정합니다.

- USER 클래스가 있어야 합니다.

  규칙은 USER 클래스에 속한 사용자를 정의합니다.

- USER 개체 mytestuser2 가 있어야 합니다.

  USER 클래스의 mytestuser2 개체가 규칙에 명시적으로 정의됩니다.

- OBJ_TYPE 속성이 있어야 합니다.

  규칙은 operator 매개 변수를 사용하여 USER 개체의 OBJ_TYPE 매개 변수를 설정합니다.

- 값 Operator 가 OBJ_TYPE 속성에 할당됩니다.

  규칙은 이 값을 명시적으로 설정합니다.

추가된 요소를 나타내는 위반

위반 계산기는 누락된 요소와 추가된 새 요소를 구별합니다. 추가된 요소는 로컬로 정의되었지만 지정된 정책에는 없는 CA Access Control 요소입니다. 이러한 추가된 요소는 클래스, 개체, 속성 및 값이 될 수 있습니다.

다음과 같은 경우 추가 위반이 포함됩니다.

- 로컬 예외로 인해 정책 내에서 설명한 개체의 속성에 새 값이 추가된 경우
- 로컬 예외로 인해 정책 내에서 설명한 개체에 새 속성이 추가된 경우

참고: 정책 내에서 설명하지 않은 새 개체는 추가 요소로 고려되지 않으며 새 클래스의 경우에도 마찬가지입니다.

수정된 요소를 나타내는 위반

수정된 요소를 표시하는 위반은 위반 데이터 파일의 어떠한 위반 줄에도 수정 사항이 표시되지 않을 때 발생합니다. 수정 사항을 식별하려면 동일한 요소에 적용되는 순차적 제거 및 추가 줄을 찾아야 합니다. 예를 들어 다음은 위반 데이터 파일에서 추출한 내용입니다. 여기에서 mytestuser 값이 Operator 에서 Auditor 및 Administrator 로 수정되었습니다.

```
DIFF, (USER), (mytestuser2), (OBJ_TYPE), -(Operator)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Auditor)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Administrator)
```

제 5 장: 권한 있는 계정 관리

이 장은 아래의 주제를 포함하고 있습니다.

권한 있는 사용자 암호 관리

권한 있는 사용자 암호 관리(PUPM)는 회사에서 가장 강력한 계정과 관련된 모든 활동을 추적하고, 관리하고, 보안을 유지하기 위한 프로세스입니다.

PUPM 을 사용하면 중앙 위치에서 대상 끝점에 있는 권한 있는 계정의 액세스 권한을 역할에 기반하여 관리할 수 있습니다. PUPM 은 권한 있는 계정 및 응용 프로그램 ID 암호를 안전하게 저장하고, 정의하는 정책에 기반하여 권한 있는 계정 및 암호에 대한 액세스를 제어합니다. 그 외에도 PUPM 을 사용하면 권한 있는 계정과 응용 프로그램 암호 수명 주기를 관리하고 구성 파일 및 스크립트에서 암호를 제거할 수 있습니다.

추가 정보:

권한 있는 계정이란?(페이지 95)

권한 있는 계정이란?

권한 있는 계정은 개별 계정에 할당되지 않고 업무에 핵심적인 데이터 및 프로세스에 액세스할 수 있는 계정입니다. 시스템 관리자는 권한 있는 계정을 사용하여 대상 끝점에서 관리 작업을 수행하거나 무인 모드에서 처리하기 위해 서비스 파일, 스크립트, 구성 파일에 관리 작업을 포함시킬 수 있습니다.

권한 있는 계정은 식별 가능한 사용자에게 할당되지 않으므로 감사 및 추적이 어렵고, 따라서 통제하는 데 어려움이 있습니다. 이로 인해 업무에 핵심적인 시스템이 실수나 악의적인 행위로 의해 손상될 수 있는 취약점이 생기게 됩니다. 회사나 조직은 업무에 차질이 없는 한도 내에서 이러한 권한 있는 계정의 수를 최소한 줄여야 합니다.

관리자(Administrator)는 기밀 정보 액세스에 대한 대부분의 내부 제어를 바이패스할 수 있으며 응용 프로그램을 삭제하거나 작용 불능 상태로 만들어 서비스 거부(DOS) 공격을 유발할 수도 있습니다. 더 나아가, 권한 있는 계정을 사용하여 수행된 이러한 작업이 실제 어떤 사용자 계정에 의해 수행되었는지 파악하기가 어렵습니다.

추가 정보:

권한 있는 사용자 암호 관리(페이지 95)

권한 있는 액세스 역할 및 권한 있는 계정

권한 있는 액세스 역할을 사용하여 각 사용자가 CA Access Control 엔터프라이즈 관리에서 수행하는 PUPM 작업과 각 사용자가 체크 인 및 체크 아웃할 수 있는 권한 있는 계정을 지정합니다. CA Access Control 엔터프라이즈 관리에는 미리 정의된 권한 있는 액세스 역할이 포함되어 있습니다. 용도에 맞게 이 미리 정의된 역할을 수정하거나 새 역할을 만들 수 있습니다.

사용자가 CA Access Control 엔터프라이즈 관리에 로그인하면 자신의 역할과 일치하는 작업 및 권한 있는 계정만 볼 수 있습니다.

추가 정보:

권한 있는 액세스 역할(페이지 23)

권한 있는 액세스 역할 사용

회사에서 PUPM 을 설정하기 전에 다음 사항을 고려해야 합니다.

- 사용자 저장소로 Active Directory 를 사용하고 Active Directory 의 그룹을 가리키도록 각 역할에 대한 구성원 정책을 수정하는 것이 좋습니다. 이 방법으로 설정하는 역할에서 사용자를 추가 또는 제거하려면 Active Directory 그룹에서 사용자를 추가 또는 제거합니다. 이렇게 하면 관리 오버헤드를 줄일 수 있습니다.

- 사용자 저장소로 Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리를 사용하여 사용자 또는 그룹을 만들거나 삭제할 수 없습니다. Active Directory 에서만 사용자 및 그룹을 만들고 삭제할 수 있습니다.
- 역할에 정의된 구성원 정책이 있고 PUPM 사용자 관리자가 사용자에게 특정 역할을 할당하지만 사용자가 구성원 정책의 범위에 맞지 않는 경우 CA Access Control 은 역할을 사용자에게 할당하지 않습니다. 구성원 정책에 정의된 규칙은 PUPM 사용자 관리자 할당보다 우선 순위가 높습니다.
- 권한 있는 계정 요청에 응답하려면 사용자에게 PUPM 승인자 역할이 있어야 하며 요청하는 사용자의 관리자여야 합니다. CA Access Control 엔터프라이즈 관리에서 사용자를 수정할 때 사용자의 관리자를 지정할 수 있습니다.
- 기본적으로 CA Access Control 은 모든 사용자에게 Break Glass, PUPM 승인자, 권한 있는 계정 요청, PUPM 사용자 역할을 할당합니다. 이 설정을 변경하려면 각 역할에 대한 구성원 정책을 수정하십시오.
- 특정 끝점 및 역할이 액세스할 수 있는 권한 있는 계정을 정의하기 위해 역할에 대한 범위 규칙을 수정할 수 있습니다. 범위 규칙을 사용하면 회사 전체에서 권한 있는 계정에 대한 세부적인 액세스를 구현할 수 있습니다. 범위 규칙은 역할의 구성원 정책에 정의됩니다.

추가 정보:

구성원 정책(페이지 28)

권한 있는 액세스 역할이 작업 체크 아웃 및 체크 인에 주는 영향

끝점에서 관리 작업을 수행하기 위해 권한 있는 계정을 체크 아웃하고 끝점에서 작업을 완료한 다음 권한 있는 계정을 체크 인합니다.

중요! 사용자에게는 끝점 유형에서 작업을 수행하기 위한 끝점 권한 있는 액세스 역할이 있어야 합니다. 끝점 권한 있는 액세스 역할은 권한 있는 액세스 계정을 사용하여 사용자가 작업을 수행할 수 있는 끝점의 유형을 지정합니다. 예를 들어, 사용자에게 Windows Agentless 끝점 권한 있는 액세스 역할을 할당하면 사용자는 권한 있는 계정을 사용하는 Windows 끝점에서 끝점 작업을 수행할 수 있습니다. Break Glass, 권한 있는 계정 요청 또는 PUPM 사용자 역할을 사용자에게 할당하는 경우 사용자에게 끝점 권한 있는 액세스 역할도 할당해야 합니다. 그렇지 않으면 사용자가 어떠한 작업도 완료할 수 없습니다.

다음 프로세스는 권한 있는 액세스 역할이 사용자가 수행하는 작업의 체크 아웃 및 체크 인에 주는 영향에 대해 설명합니다.

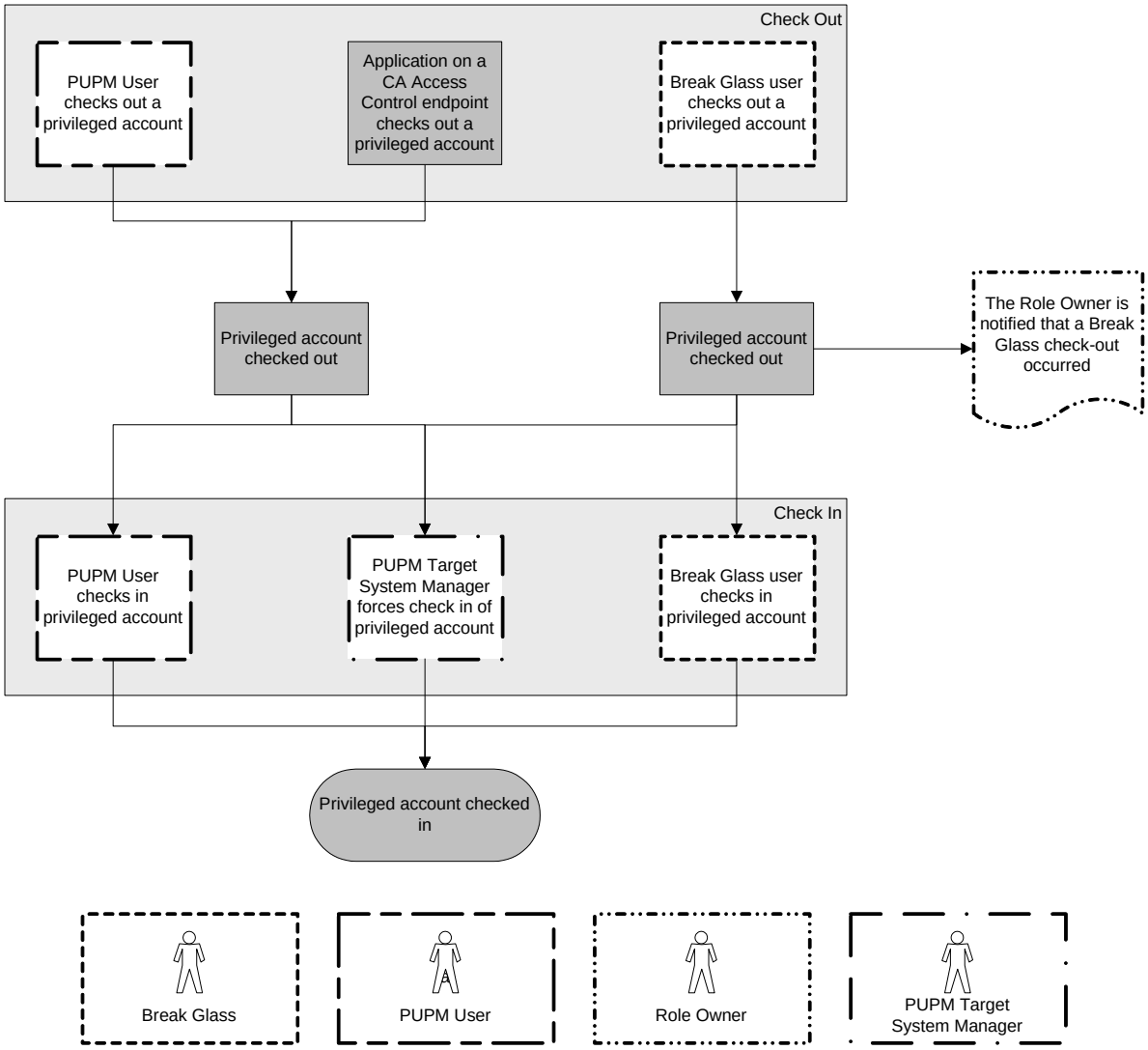
1. 사용자는 다음 방법 중 하나를 사용하여 권한 있는 계정을 체크 아웃합니다.
   - PUPM 사용자 역할이 있는 사용자가 권한 있는 계정을 체크 아웃합니다.
   - Break Glass 역할이 있는 사용자가 break glass 체크 아웃을 수행합니다.
   - CA Access Control 끝점에 있는 응용 프로그램이 권한 있는 계정을 체크 아웃합니다.

   권한 있는 계정이 체크 아웃됩니다.

   참고: 사용자가 break glass 체크 아웃을 수행하면 CA Access Control 은 역할 소유자에게 알림 메시지를 보냅니다. 역할 소유자는 감사를 위해 이 메시지에 추가 정보를 추가할 수 있습니다.
2. 사용자는 다음 방법 중 하나를 사용하여 권한 있는 계정을 체크 인합니다.
   - PUPM 사용자 역할이 있는 사용자가 권한 있는 계정을 체크 인합니다.
   - Break Glass 역할이 있는 사용자가 권한 있는 계정을 체크 인합니다.
   - CA Access Control 끝점에 있는 응용 프로그램이 권한 있는 계정을 체크 인합니다.
   - PUPM 대상 시스템 관리자 역할이 있는 사용자가 권한 있는 계정을 강제로 체크 인합니다.

   권한 있는 계정이 체크 인됩니다.

다음 다이어그램은 권한 있는 액세스 역할이 사용자가 수행하는 작업의 체크 인 및 체크 아웃에 주는 영향을 설명합니다.



예: 권한 있는 계정 체크 아웃

본인에게 시스템 관리자 역할이 있습니다. Joe 에게 PUPM 사용자 역할과 Windows Agentless 연결 끝점 권한 있는 액세스 역할을 할당합니다. Joe 가 CA Access Control 엔터프라이즈 관리에 로그인하고 Windows 끝점에서 권한 있는 계정을 체크 아웃하고 체크 인할 수 있는 작업만 살펴봅니다.

예: 권한 있는 계정에 대한 Break Glass

본인에게 시스템 관리자 역할이 있습니다. Fiona 에게 Break Glass 역할과 Oracle 서버 연결 끝점 권한 있는 액세스 역할을 할당합니다. Fiona 는 Oracle 끝점에 즉시 액세스해야 합니다. Fiona 가 CA Access Control 엔터프라이즈 관리에 로그인하여 Oracle 끝점에서 계정에 대한 break glass 체크 아웃을 수행할 수 있는 작업만 살펴봅니다. Fiona 는 Oracle 권한 있는 계정에 대해 break glass 체크 아웃을 수행하고 CA Access Control 은 Break Glass 역할 소유자에게 알림 메시지를 보냅니다.

참고: 기본적으로 Break Glass 역할 소유자는 시스템 관리자 관리 역할입니다.

권한 있는 액세스 역할이 권한 있는 계정 요청 작업에 주는 영향

사용자가 권한 있는 계정을 체크 아웃할 수 없고 계정에 즉시 액세스할 필요가 없는 경우 사용자는 권한 있는 계정 요청을 제출할 수 있습니다. 사용자의 관리자는 권한 있는 계정 요청을 승인 또는 거부할 수 있습니다. 이 항목에서는 사용자가 권한 있는 계정 요청 작업을 수행하기 위해 필요한 권한 있는 액세스 역할에 대해 설명합니다.

중요! 사용자에게는 끝점 유형에서 작업을 수행하기 위한 끝점 권한 있는 액세스 역할이 있어야 합니다. 끝점 권한 있는 액세스 역할은 권한 있는 액세스 계정을 사용하여 사용자가 작업을 수행할 수 있는 끝점의 유형을 지정합니다. 예를 들어, 사용자에게 Windows Agentless 끝점 권한 있는 액세스 역할을 할당하면 사용자는 권한 있는 계정을 사용하는 Windows 끝점에서 끝점 작업을 수행할 수 있습니다. Break Glass, 권한 있는 계정 요청 또는 PUPM 사용자 역할을 사용자에게 할당하는 경우 사용자에게 끝점 권한 있는 액세스 역할도 할당해야 합니다. 그렇지 않으면 사용자가 어떠한 작업도 완료할 수 없습니다.

다음 프로세스는 권한 있는 액세스 역할이 사용자가 수행할 수 있는 권한 있는 액세스 요청 작업에 주는 영향에 대해 설명합니다.

1. 권한 있는 액세스 요청 역할이 있는 사용자가 권한 있는 계정에 대한 액세스를 요청합니다.
2. CA Access Control 은 권한 있는 계정 요청을 사용자의 관리자(PUPM 승인자 역할도 필요함)에게 보냅니다.

   참고: 권한 있는 계정 요청을 받으려면 PUPM 승인자 역할이 있어야 하는 동시에 해당 사용자의 관리자여야 합니다.

3. PUPM 승인자 역할이 있는 사용자가 권한 있는 계정 요청에 응답하고 다음 중 하나를 수행합니다.

   - 권한 있는 계정 요청을 거부합니다.

     권한 있는 계정 요청 역할이 있는 사용자가 권한 있는 계정을 체크 아웃할 수 없습니다.

   - 권한 있는 계정 요청을 예약합니다.

     다른 사용자가 이 권한 있는 계정 요청을 승인 또는 거부할 수 없습니다. PUPM 승인자가 요청을 승인할 때까지 권한 있는 계정 요청 역할이 있는 사용자가 권한 있는 계정을 체크 아웃할 수 없습니다.

   - 권한 있는 계정 요청을 승인합니다.

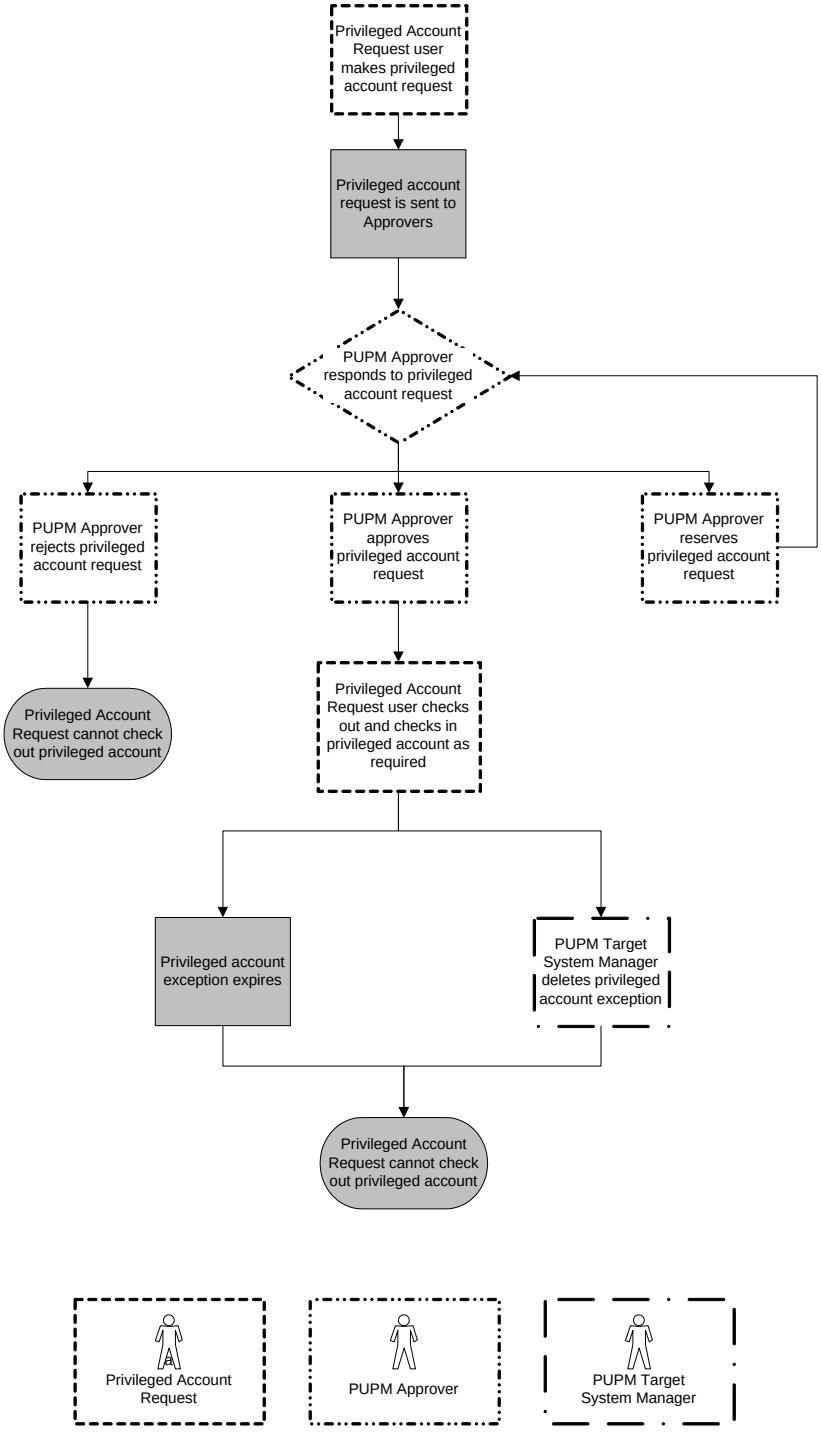
     권한 있는 요청 역할이 있는 사용자에게 권한 있는 계정 예외가 부여되어 사용자가 권한 있는 계정을 체크 아웃 및 체크 인할 수 있습니다.

4. 다음 이유 중 하나로 인해 권한 있는 계정 예외가 만료됩니다.

   - 권한 있는 계정 예외에 지정된 만료 시간에 도달했습니다.
   - PUPM 대상 시스템 관리자 역할이 있는 사용자가 권한 있는 계정 예외를 삭제했습니다.

   권한 있는 계정 요청 역할이 있는 사용자가 더 이상 권한 있는 계정을 체크 아웃할 수 없습니다.

다음 다이어그램은 권한 있는 액세스 역할이 사용자가 수행할 수 있는 권한 있는 액세스 요청 작업에 주는 영향에 대해 설명합니다.



예: 권한 있는 계정 요청 및 이 요청에 응답

본인에게 시스템 관리자 역할이 있습니다. Alice 에게 권한 있는 계정 요청 역할과 SSH 장치 연결 끝점 권한 있는 액세스 역할을 할당합니다. Alice 의 관리자인 Bob 에게 PUPM 승인자 역할을 할당합니다.

Alice 가 CA Access Control 엔터프라이즈 관리에 로그인하고 UNIX 끝점의 계정에 대한 권한 있는 계정 요청을 제출할 수 있는 작업만 살펴봅니다. Alice 가 UNIX 끝점의 example_ux 계정에 대한 권한 있는 계정 요청을 제출합니다.

Bob 이 CA Access Control 엔터프라이즈 관리에 로그인하여 권한 있는 계정 요청에 응답할 수 있는 작업만 살펴봅니다. Bob 이 Alice 의 권한 있는 액세스 요청을 승인하고 권한 있는 계정 예외가 오후 6 시까지 유효하도록 지정합니다. Alice 는 이제 example_ux 권한 있는 계정에 체크 인 및 체크 아웃할 수 있습니다. 오후 6 시에 권한 있는 계정 예외가 만료되고 Alice 는 더 이상 example_ux 권한 있는 계정을 체크 아웃할 수 없게 됩니다.

권한 있는 계정 설정 방법

권한 있는 계정 암호를 사용하려면 먼저 PUPM 에 대해 CA Access Control 엔터프라이즈 관리를 설정하는 일부 단계를 완료해야 합니다. 그런 다음 사용자들이 정의된 권한 있는 계정을 사용하여 작업을 시작할 수 있게 됩니다.

참고: CA Access Control 엔터프라이즈 관리를 설치하면 배포 서버의 일부로서 기본 JCS(Java Connector Server)를 설치하고 구성합니다. CA Access Control 끝점 유형으로 PUPM 을 사용하려면 먼저 JCS(Java Connector Server)가 설치되고 구성되어 있어야 합니다. CA Identity Manager 커넥터를 사용하여 작업하려면 Identity Manager 프로비저닝 유형의 커넥터 서버를 만들어야 합니다.

다음 프로세스는 권한 있는 계정을 설정하기 위해 회사의 사용자들이 반드시 완료해야 하는 작업에 대해 설명합니다. 사용자에게는 각 프로세스 단계를 완료하기 위한 지정된 역할이 있어야 합니다.

참고: 시스템 관리자 관리 역할이 있는 사용자는 이 프로세스에서 모든 작업을 수행할 수 있습니다.

권한 있는 계정을 설정하려면 사용자가 다음을 수행해야 합니다.

1. 시스템 관리자가 CA Access Control 엔터프라이즈 관리에 끝점을 만듭니다.

   끝점은 권한 있는 계정이 관리하는 장치입니다.

2. PUPM 대상 시스템 관리자가 암호 정책을 만듭니다.

   암호 정책은 권한 있는 계정에 대한 암호 규칙 및 제한을 설정합니다.

3. PUPM 대상 시스템 관리자가 각 끝점에서 권한 있는 계정을 검색하고 권한 있는 계정을 만들지 여부를 선택합니다.

   권한 있는 계정을 검색하면 CA Access Control 엔터프라이즈 관리가 이 계정을 관리할 수 있게 만듭니다.

4. (선택 사항) PUPM 대상 시스템 관리자가 추가 권한 있는 계정을 만듭니다.

   예: 연결 해제된 시스템의 권한 있는 계정

5. (선택 사항) 시스템 관리자가 CA Access Control 끝점을 위한 응용 프로그램을 만듭니다.

   이 응용 프로그램을 사용하여 PUPM 에이전트가 필요할 때만 가져오는 권한 있는 계정 암호로 스크립트에 있는 하드 카피 암호를 대체할 수 있습니다.

6. PUPM 정책 관리자가 권한 있는 액세스 역할의 구성원 정책을 수정합니다.

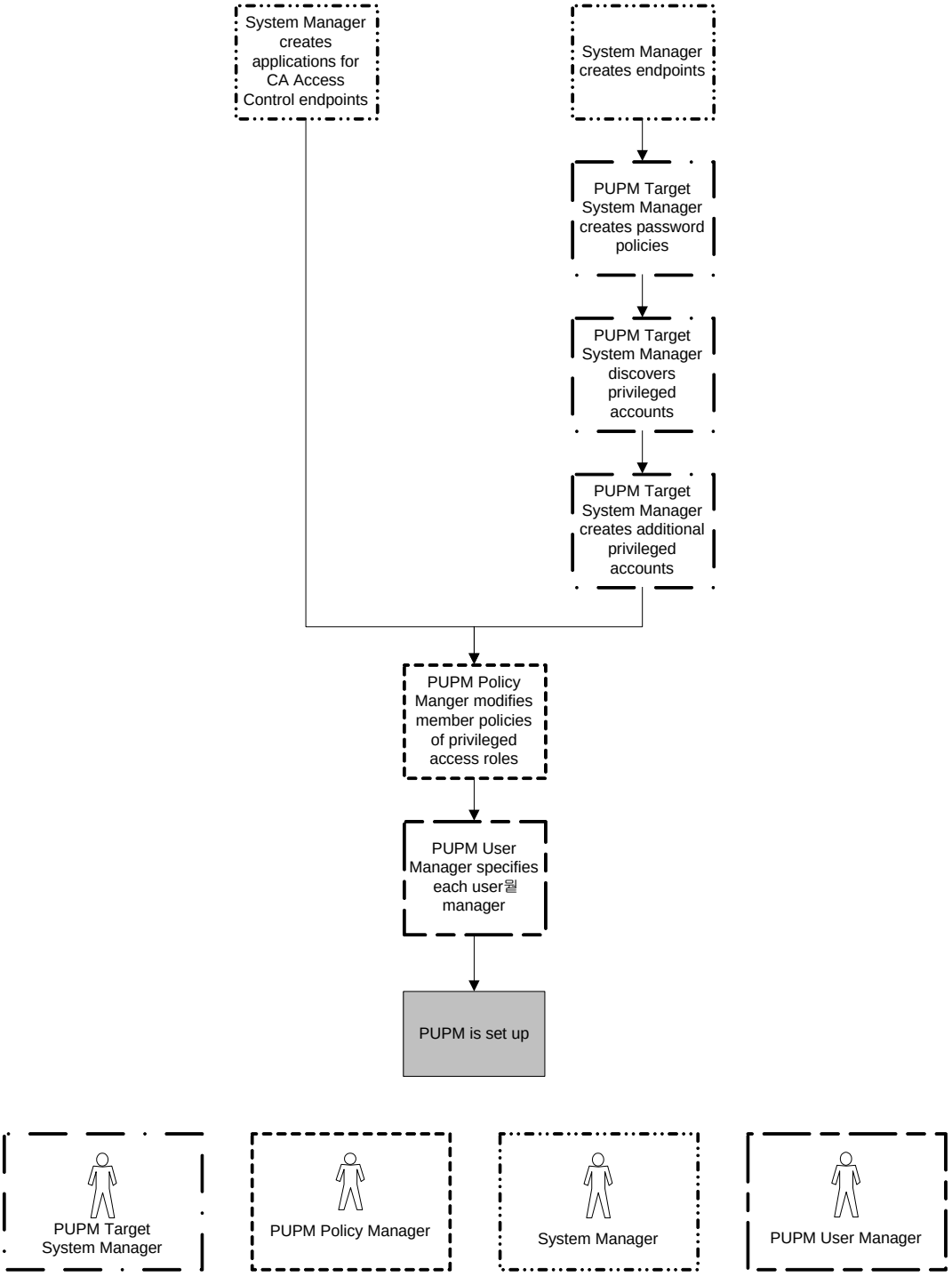
   구성원 정책은 역할에서 작업을 수행할 수 있는 사용자를 정의합니다.

   참고: 사용자 저장소로 Active Directory 를 사용하는 경우 해당 Active Directory 그룹을 가리키도록 각 구성원 정책을 수정하는 것이 좋습니다. 그런 다음 해당 Active Directory 그룹에서 추가 또는 제거하는 방법으로 역할에서 사용자를 추가 또는 제거할 수 있습니다. 이렇게 하면 관리 오버헤드를 크게 줄일 수 있습니다.

7. (포함된 사용자 저장소) PUPM 사용자 관리자는 각 사용자의 관리자를 지정합니다.

   사용자의 관리자만 사용자의 권한 있는 계정 요청을 승인할 수 있습니다.

다음 다이어그램은 각 프로세스 단계를 수행하는 권한 있는 액세스 역할을 설명합니다.



끝점 유형 보기

끝점 유형은 지원되는 관리 시스템에 대한 CA Access Control 엔터프라이즈 관리의 기존 정의입니다. 각 끝점 유형은 권한 있는 계정이 있는 시스템의 유형을 지정합니다.

끝점 유형을 보려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "끝점", "끝점 유형 보기"를 클릭합니다.

   "끝점 유형 보기: 끝점 유형 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 끝점 유형의 목록이 나타납니다. 다음은 CA Access Control 엔터프라이즈 관리가 지원하는 끝점 유형입니다.

끝점 만들기

CA Access Control 엔터프라이즈 관리에 끝점 정의를 만들면 끝점을 관리하고 끝점에 있는 권한 있는 계정을 검색할 수 있습니다.

끝점을 만들려면

참고: 권한 있는 계정을 관리하려면 관리 권한이 있어야 합니다.

1. "권한 있는 계정", "끝점", "끝점 만들기"를 차례로 선택합니다.

   "끝점 만들기" 검색 화면이 나타납니다.

2. 끝점을 만들도록 선택한 다음 "확인"을 클릭합니다.

   "끝점 만들기" 화면이 나타납니다.

3. 다음 매개 변수를 입력합니다.

   이름

   끝점 이름을 정의합니다.

   설명

   끝점의 일반 텍스트 설명을 정의합니다.

   끝점 유형

   권한 있는 계정이 있는 끝점의 유형을 지정합니다.

   선택 사항: MS SQL Server(Microsoft SQL Server), PeopleSoft, OS400(IBM i, 이전 이름: i5/OS 및 OS/400), Kerberos 서버, Oracle Server, Windows Agentless, SSH 장치

특정 호스트

사용자 로그인 이름을 정의합니다.

예: administrator

암호

사용자 계정의 암호를 정의합니다.

URL

끝점 유형별로 끝점에 대한 URL 을 정의합니다.

예: ssh://computer_name.com

호스트

호스트의 정규화된 이름을 정의합니다.

4. "제출"을 클릭합니다.

끝점이 만들어집니다.

MS SQL Server 연결 정보

MS SQL Server 끝점 유형을 사용하면 권한 있는 Microsoft SQL Server 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

URL

CA Access Control 엔터프라이즈 관리가 끝점에 연결하기 위해 사용할 수 있는 URL 을 정의합니다. URL 은 데이터베이스 서버의 특정 유형을 지정합니다.

형식: jdbc:microsoft:sqlserver://servername:port

예: jdbc:microsoft:sqlserver://localhost:1433

참고: URL 의 형식에 대한 자세한 내용은 끝점 설명서를 참조하십시오.

호스트

끝점의 호스트 이름을 정의합니다.

고급

끝점에 대한 관리되는 계정으로 다른 관리 계정을 사용할지 여부를 지정합니다.

이 옵션을 지정하면 끝점에 연결하기 위해 사용자가 제공했던 계정 정보 대신 CA Access Control 엔터프라이즈 관리가 사용하는 계정을 정의합니다.

PeopleSoft 연결 정보

PeopleSoft 끝점 유형을 사용하면 권한 있는 PeopleSoft Enterprise 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

고급

끝점에 대한 관리되는 계정으로 다른 관리 계정을 사용할지 여부를 지정합니다.

이 옵션을 지정하면 끝점에 연결하기 위해 사용자가 제공했던 계정 정보 대신 CA Access Control 엔터프라이즈 관리가 사용하는 계정을 정의합니다.

OS400 연결 정보

OS400 끝점 유형을 사용하면 권한 있는 IBM i(이전 이름: i5/OS 및 OS/400) 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

URL

CA Access Control 엔터프라이즈 관리가 끝점에 연결하기 위해 사용할 수 있는 URL 을 정의합니다. URL 은 데이터베이스 서버의 특정 유형을 지정합니다.

형식: jdbc:as400://host;proxy server=ServerName:proxyServerPort

예: jdbc:as400://myiSeries;proxy server=myHODServer:3470

참고: URL 의 형식에 대한 자세한 내용은 끝점 설명서를 참조하십시오.

호스트

끝점의 호스트 이름을 정의합니다.

고급

끝점에 대한 관리되는 계정으로 다른 관리 계정을 사용할지 여부를 지정합니다.

이 옵션을 지정하면 끝점에 연결하기 위해 사용자가 제공했던 계정 정보 대신 CA Access Control 엔터프라이즈 관리가 사용하는 계정을 정의합니다.

Kerberos 서버 연결 정보

Kerberos 서버 끝점 유형을 사용하면 권한 있는 Kerberos 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

고급

끝점에 대한 관리되는 계정으로 다른 관리 계정을 사용할지 여부를 지정합니다.

이 옵션을 지정하면 끝점에 연결하기 위해 사용자가 제공했던 계정 정보 대신 CA Access Control 엔터프라이즈 관리가 사용하는 계정을 정의합니다.

Oracle 서버 연결 정보

Oracle 서버 끝점 유형을 사용하면 권한 있는 Oracle 데이터베이스 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

URL

CA Access Control 엔터프라이즈 관리가 끝점에 연결하기 위해 사용할 수 있는 URL 을 정의합니다. URL 은 데이터베이스 서버의 특정 유형을 지정합니다.

형식: jdbc:oracle:drivertype:@hostname:port/service

예: jdbc:oracle:thin:@ora.comp.com:1521/orcl

참고: URL 의 형식에 대한 자세한 내용은 끝점 설명서를 참조하십시오.

호스트

끝점의 호스트 이름을 정의합니다. 이 이름은 정규화된 호스트 이름입니다.

고급

끝점에 대한 관리되는 계정으로 다른 관리 계정을 사용할지 여부를 지정합니다.

이 옵션을 지정하면 끝점에 연결하기 위해 사용자가 제공했던 계정 정보 대신 CA Access Control 엔터프라이즈 관리가 사용하는 계정을 정의합니다.

Windows Agentless 연결 정보

Windows Agentless 끝점 유형을 사용하면 권한 있는 Windows 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

예: myhost-ac-1

호스트 도메인

이 호스트가 구성원으로 포함된 도메인 이름을 지정합니다.

참고: 호스트 도메인 이름은 접두사만 사용하여 지정하십시오. 예를 들어, 전체 도메인 이름이 company.com 인 경우 접두사인 company 만 입력합니다.

Active Directory

사용자 계정이 Active Directory 계정인지 여부를 지정합니다.

제한: true, false

사용자 도메인

사용자가 구성원으로 포함된 도메인 이름을 지정합니다.

참고: 사용자 도메인 이름은 접두사만 사용하여 지정하십시오. 예를 들어, 전체 도메인 이름이 company.com 인 경우 접두사인 company 만 입력합니다.

고급

끝점에 대한 관리되는 계정으로 다른 관리 계정을 사용할지 여부를 지정합니다.

이 옵션을 지정하면 끝점에 연결하기 위해 사용자가 제공했던 계정 정보 대신 CA Access Control 엔터프라이즈 관리가 사용하는 계정을 정의합니다.

SSH 장치 연결 정보

SSH 장치 유형을 사용하면 권한 있는 UNIX 계정을 관리할 수 있습니다.

이 유형의 장치를 만들 때는 CA Access Control 엔터프라이즈 관리가 장치에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

구성 파일

정의하는 SSH 장치 XML 구성 파일의 이름을 지정합니다.

고급

끝점에 대한 관리되는 계정으로 다른 관리 계정을 사용할지 여부를 지정합니다.

이 옵션을 지정하면 끝점에 연결하기 위해 사용자가 제공했던 계정 정보 대신 CA Access Control 엔터프라이즈 관리가 사용하는 계정을 정의합니다.

SSH 장치 XML 파일 사용자 지정

권한 있는 계정을 검색하기 위해 PUPM 이 사용하는 기본 설정이 사용하는 SSH 장치에 적용되지 않는 경우 필요에 맞게 SSH 장치 XML 파일을 사용자 지정할 수 있습니다.

SSH 장치 XML 파일을 사용자 지정하려면

1. CA Access Control 엔터프라이즈 관리에서 ssh_connector_conf.xml 파일을 찾습니다. 이 파일은 기본적으로 다음 위치에 있습니다.

   ```
   \Program Files\CA\AccessControlServer\Connector Server\conf\override\sshdyn\
   ```

2. 이 파일을 복사하여 새 이름으로 저장합니다.

   참고: 새 파일은 원래 파일이 있는 동일한 디렉터리에 저장하십시오.

3. 편집 가능한 형식으로 만든 파일을 엽니다.
4. 필요에 맞게 매개 변수를 수정하고 파일을 저장합니다.
5. CA Access Control 엔터프라이즈 관리에 SSH 장치 끝점을 만듭니다(페이지 106).
6. "구성" 필드에 만든 XML 파일의 이름을 입력합니다.

   사용자 지정 설정을 사용하여 SSH 장치 끝점이 만들어집니다.

7. 만든 끝점에서 권한 있는 계정 검색 마법사(페이지 118)를 실행합니다.

   CA Access Control 엔터프라이즈 관리가 XML 파일에서 정의한 매개 변수를 사용하여 끝점에서 권한 있는 계정을 검색합니다.

8. JCS 커넥터 로그 파일(jcs_stdout.log)과 JCS 커넥터 오류 파일(jcs_sterr.log)을 검토합니다. 기본적으로 이 파일들은 다음 위치에 있습니다.

   ```
   \Program Files\CA\AccessControlServer\Connector Server\logs\
   ```

9. 필요하면 로그 파일에 표시된 오류를 해결하기 위해 XML 파일을 수정합니다.

예: SSH 장치 XML 파일 사용자 지정

이 예는 필요에 맞게 SSH 장치 XML 파일을 사용자 지정하는 방법을 보여줍니다. 이 예에서 관리자는 사용자 계정을 검색하기 위해 PUPM 이 실행하는 명령에 대한 매개 변수를 수정하고 끝점에서 암호를 변경하기 위한 매개 변수를 수정합니다.

관리자가 사용자 계정을 검색하기 위해 PUPM 가 실행한 명령(oGetUsers)에 대한 만료 기간을 1000 밀리초로 수정했습니다. 그런 다음, 관리자는 계정 암호를 변경하기 위해 PUPM 이 실행하는 명령(oChangePassword)의 만료 기간을 1500 밀리초로 수정했습니다. 마지막으로 관리자는 계정 암호를 사용자에게 표시하는 기간(sWaitForText) 1000 밀리초로 수정했습니다.

```
<array name="oGetUsers">

        <item>

          <param name="sCommand" value="echo" />

          <param name="iWait" value="1000" />

        </item>

        <item>

        <param name="sCommand" value="cat /etc/passwd | cut -d: -f1 | grep -w
[%%filter%%]" />

            <param name="iWait" value="1000" />

        </item>

        </array>

                <array name="oChangePassword">

        <item>

           <param name="sCommand" value="echo" />

           <param name="iWait" value="1500" />

        </item>

        <item>

        <param name="sCommand" value="passwd [%%user%%]" />

           <param name="iWait" value="1000" />

           <param name="sWaitForText" value="word:" />

        </item>
```

CA Identity Manager 프로비저닝 연결 정보

CA Identity Manager 프로비저닝 커넥터를 사용하면 프로비저닝 서버에서 정의한 CA Identity Manager 끝점을 관리할 수 있습니다.

참고: CA Access Control 엔터프라이즈 관리를 설치하면 배포 서버의 일부로서 기본 JCS(Java Connector Server)를 설치하고 구성합니다. CA Access Control 끝점 유형으로 PUPM 을 사용하려면 먼저 JCS(Java Connector Server)가 설치되고 구성되어 있어야 합니다. CA Identity Manager 커넥터를 사용하여 작업하려면 Identity Manager 프로비저닝 유형의 커넥터 서버를 만들어야 합니다. 모든 CA Identity Manager 끝점 유형은 동일한 연결 정보를 사용합니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

끝점

CA Identity Manager 프로비저닝 서버에 정의한 그대로 끝점의 이름을 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다. 이 이름은 이 끝점에 할당하려는 논리적 이름입니다. CA Access Control 엔터프라이즈 관리는 이 이름을 사용하여 월드 뷰에서 끝점을 나타냅니다.

고급

끝점에 대한 관리되는 계정으로 다른 관리 계정을 사용할지 여부를 지정합니다.

이 옵션을 지정하면 끝점에 연결하기 위해 사용자가 제공했던 계정 정보 대신 CA Access Control 엔터프라이즈 관리가 사용하는 계정을 정의합니다.

암호 정책 만들기

권한 있는 계정에 대한 암호 정책은 권한 있는 계정의 허용되는 암호를 결정하는 일련의 규칙 및 제한입니다. 예를 들어, 길이가 8 자 이상이고 숫자 및 문자를 포함하도록 암호를 규정하는 정책을 구성할 수 있습니다. 암호 정책은 또한 CA Access Control 엔터프라이즈 관리가 계정에 대한 새 암호를 자동으로 만드는 간격을 결정합니다.

참고: CA Access Control 엔터프라이즈 관리에는 미리 정의된 암호 정책이 포함되어 있습니다. 회사의 보안 요구 사항을 충족하고 각 끝점에 적절한 암호 정책을 정의하여 사용하는 것이 좋습니다.

암호 정책을 만들려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "암호 정책", "암호 정책 만들기"를 차례로 클릭합니다.

   "암호 정책 만들기: 표준 검색 구성 화면" 페이지가 나타납니다.

2. (선택 사항) 다음과 같이 암호 정책을 만들 때 복사하여 사용할 기존 암호 정책을 선택합니다.

   a. "권한 있는 계정" 유형의 개체 복사본 만들기를 선택한 다음 "검색"을 클릭합니다.

      암호 정책의 목록이 표시됩니다.

   b. 새 암호 정책을 만들 때 기초로 사용할 개체를 선택합니다.

3. "확인"을 클릭합니다.

   "암호 정책 만들기" 작업 페이지가 나타납니다. 기존 개체에서 암호 정책을 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.

4. 암호 정책의 이름과 선택적 설명을 입력합니다.

5. (선택 사항) 활성화 표시를 지웁니다.

   기본적으로 새 암호 정책은 활성화되어 있습니다. 만들고 있는 정책이 아직 승인되지 않은 경우 비활성화된 상태로 둘 수 있습니다.

6. 암호 조합 규칙을 정의합니다.

7. (선택 사항) 암호 만료 간격을 정의합니다.

   이 간격은 CA Access Control 엔터프라이즈 관리가 암호를 자동으로 변경하는 일반 간격입니다. 기본적으로 만료 간격은 비활성화(0 으로 설정)되어 있습니다.

8. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 암호 정책을 만듭니다.

추가 정보:

암호 조합 규칙(페이지 116)

암호 조합 규칙

암호 정책을 만들 때 새 암호에 대한 내용 요구 사항을 정의할 수 있습니다.

중요! 암호 조합 규칙을 구성하는 경우 문자 요구 사항의 값을 결정할 때 최대 암호 길이를 사용하는 것이 좋습니다. 필요한 문자 또는 숫자의 총 수가 최대 암호 길이를 초과하면 모든 암호가 거부됩니다.

CA Access Control 엔터프라이즈 관리는 권한 있는 계정에 대한 다음과 같은 암호 조합 규칙을 제공합니다.

최소 암호 길이

암호에 들어가야 하는 문자의 최소 수를 정의합니다.

최대 암호 길이

암호에 들어갈 수 있는 문자의 최대 수를 정의합니다.

최대 반복 문자

암호에 들어갈 수 있는 반복되는 문자의 최대 수를 정의합니다.

예를 들어, 이 값을 3 으로 설정하면 문자열 "aura"는 암호에 사용될 수 없지만 "aura"는 사용될 수 있습니다.

대문자(패턴: u)

암호에 대문자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 대문자 수를 정의합니다.

소문자(패턴: c)

암호에 소문자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 소문자 수를 정의합니다.

문자(패턴: l)

암호에 영문자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 영문자 수를 정의합니다.

숫자(패턴: d)

암호에 숫자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 숫자 수를 정의합니다.

문자 또는 숫자(패턴: a)

암호에 영숫자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 영숫자 수를 정의합니다.

문장 부호(패턴: p)

암호에 문장 부호 또는 특수 문자(비영숫자)를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 이러한 문자 수를 정의합니다.

모두(패턴: *)

암호가 모든 문자를 포함할 수 있도록 지정합니다. 이 옵션을 선택하면 CA Access Control 엔터프라이즈 관리는 자동으로 다른 모든 문자 내용 정의를 선택합니다.

패턴 사용

문자 내용 정의를 정의하는 대신 암호에 반드시 사용해야 하는 패턴을 정의하도록 지정합니다.

예:

- **uuuuu** - ASDKF 또는 IUTYE 에 일치
- **ucdddp** - Rv671* 또는 Uc194^에 일치
- ******** - lkI&5Jj@ 또는 sffIU*&1 에 일치
- **lllaaaa** - yuUI1Uo3 또는 qWcV1Er6 에 일치

금지된 문자

권한 있는 계정 암호를 만들거나 수정할 때 사용할 수 없는 문자를 정의합니다.

권한 있는 계정 검색

끝점에서 권한 있는 계정을 검색할 때는 권한 있는 계정 검색 프로세스를 지정된 간격으로 실행하는 것이 좋습니다.

참고: 끝점 유형에서 권한 있는 계정을 처음 발견했을 때 CA Access Control 엔터프라이즈 관리는 해당 끝점 유형에서 권한 있는 계정을 사용하기 위한 끝점 권한 있는 액세스 역할을 자동으로 만듭니다. 예를 들어, Windows 끝점에서 권한 있는 계정을 처음 발견했을 때 CA Access Control 엔터프라이즈 관리는 자동으로 Windows Agentless 연결 끝점 권한 있는 액세스 역할을 만듭니다.

권한 있는 계정을 검색하려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "계정", "권한 있는 계정 검색 마법사"를 클릭합니다.

   "권한 있는 계정 검색 마법사: 권한 있는 계정 선택" 페이지가 나타납니다.

2. 목록에서 "끝점 유형"을 선택합니다.
3. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 끝점의 목록이 표시됩니다.

4. 관리할 권한 있는 계정을 선택합니다.

   다음 표의 열 제목은 직관적으로 이해되지 않습니다.

   검색된 계정

   계정이 이미 CA Access Control 엔터프라이즈 관리에 알려져 있는지 여부를 지정합니다. 알려진 계정에는 CA Access Control 엔터프라이즈 관리가 이미 관리하는 계정과 CA Access Control 엔터프라이즈 관리가 끝점을 관리하기 위해 사용하는 관리자 계정을 포함합니다.

   끝점 관리자

   CA Access Control 엔터프라이즈 관리가 끝점을 관리하기 위해 계정을 사용하는지 여부를 지정합니다.

   중요! 끝점 관리자 계정을 선택하지 마십시오. CA Access Control 엔터프라이즈 관리는 관리하는 권한 있는 계정의 암호를 자동으로 변경합니다. 끝점 관리자 계정을 선택하면 끝점에 있는 권한 있는 계정에 로그인하여 관리할 수 없게 됩니다. 예를 들어, UNIX 끝점을 정의하고 root 계정을 끝점 관리자 계정으로 지정하는 경우 root 를 관리되는 권한 있는 계정으로 선택하지 마십시오.

   "다음"을 클릭합니다.

   "권한 있는 계정 검색 마법사: 일반 계정 세부 정보" 페이지가 나타납니다.

5. 대화 상자의 필드를 입력합니다. 다음 필드는 자동으로 채워지지 않습니다.

   연결 해제된 시스템

   계정이 연결 해제된 시스템에 있는지 여부를 지정합니다.

   이 옵션을 선택하면 PUPM 이 해당 계정을 관리하지 않습니다. 대신, 연결 해제된 시스템의 권한 있는 계정을 위한 암호 저장소의 역할만 수행합니다. 암호를 변경할 때마다 관리되는 끝점에서도 계정 암호를 직접 변경해야 합니다.

   암호 정책

   권한 있는 계정에 적용할 암호 정책을 지정합니다.

   체크 아웃 만료

   체크 아웃 계정이 만료되는 기간(분)을 정의합니다.

   배타적 계정

   한 번에 하나의 사용자만 계정에 액세스할 수 있는지 여부를 지정합니다. 배타적 계정은 한 번에 하나의 사용자만 권한 있는 계정을 사용하도록 제한합니다.

체크 아웃 시 암호 변경

CA Access Control 엔터프라이즈 관리가 권한 있는 계정을 체크 아웃할 때마다 이 계정 암호를 변경할지 여부를 지정합니다.

체크 인 시 암호 변경

사용자 또는 프로그램이 권한 있는 계정을 체크 인할 때마다 또는 체크 아웃 기간이 만료될 때 CA Access Control 엔터프라이즈 관리가 이 계정 암호를 변경할지 여부를 지정합니다.

참고: 배타적 계정이 아닌 경우 CA Access Control 엔터프라이즈 관리는 모든 사용자가 계정을 체크 인한 경우에만 새 권한 있는 계정 암호를 생성합니다.

"마침"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 이 작업을 제출하고 오류가 없는 경우 선택된 권한 있는 계정을 만듭니다.

권한 있는 계정 만들기

CA Access Control 엔터프라이즈 관리의 권한 있는 계정을 사용하면 사용자에게 핵심적인 데이터 및 프로세스에 액세스할 수 있는 권한 있는 시스템 계정에 대한 액세스 권한을 제공할 수 있습니다. 시스템 관리자는 권한 있는 계정을 사용하여 대상 끝점에서 관리 작업을 수행합니다.

권한 있는 계정을 만들려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "계정", "권한 있는 계정 만들기"를 클릭합니다.

   "권한 있는 계정 만들기: 권한 있는 계정 선택" 페이지가 나타납니다.

2. (선택 사항) 다음과 같이 권한 있는 계정을 만들 때 복사하여 사용할 기존 권한 있는 계정을 선택합니다.

   a. "권한 있는 계정" 유형의 개체에 대한 복사본을 만들도록 선택합니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

   c. 새로운 권한 있는 계정을 만들 때 기초로 사용할 개체를 선택합니다.

3. "확인"을 클릭합니다.

   "권한 있는 계정 만들기" 작업 페이지가 나타납니다. 기존 개체에서 권한 있는 계정을 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.

4. 대화 상자에서 다음 필드를 채웁니다.

연결 해제된 시스템

계정이 연결 해제된 시스템에 있는지 여부를 지정합니다.

이 옵션을 선택하면 PUPM 이 해당 계정을 관리하지 않습니다. 대신, 연결 해제된 시스템의 권한 있는 계정을 위한 암호 저장소의 역할만 수행합니다. 암호를 변경할 때마다 관리되는 끝점에서도 계정 암호를 직접 변경해야 합니다.

끝점 유형

권한 있는 계정이 있는 끝점의 유형을 지정합니다.

선택 사항: MS SQL Server(Microsoft SQL Server), PeopleSoft, OS400(IBM i, 이전 이름: i5/OS 및 OS/400), Kerberos 서버, Oracle Server, Windows Agentless, SSH 장치

끝점 이름

권한 있는 계정이 있는 정의된 끝점의 이름을 지정합니다. CA Access Control 엔터프라이즈 관리는 지정한 유형의 끝점만 나열합니다.

컨테이너

권한 있는 계정에 대한 컨테이너의 이름을 지정합니다. 컨테이너는 인스턴스가 다른 개체의 컬렉션인 클래스입니다. 컨테이너는 특정 액세스 규칙에 따라 개체를 체계적인 방식으로 저장하기 위해 사용됩니다.

계정 이름

이 권한 있는 계정에 대한 이름을 정의합니다.

암호

새 권한 있는 계정에 사용할 암호를 정의하고 검사합니다.

참고: 새 암호는 지정하는 암호 정책을 준수해야 합니다.

암호 정책

권한 있는 계정에 적용할 암호 정책을 지정합니다.

체크 아웃 만료

체크 아웃 계정이 만료되는 기간(분)을 정의합니다.

배타적 계정

한 번에 하나의 사용자만 계정에 액세스할 수 있는지 여부를 지정합니다. 배타적 계정은 한 번에 하나의 사용자만 권한 있는 계정을 사용하도록 제한합니다.

체크 아웃 시 암호 변경

CA Access Control 엔터프라이즈 관리가 권한 있는 계정을 체크 아웃할 때마다 이 계정 암호를 변경할지 여부를 지정합니다.

체크 인 시 암호 변경

사용자 또는 프로그램이 권한 있는 계정을 체크 인할 때마다 또는 체크 아웃 기간이 만료될 때 CA Access Control 엔터프라이즈 관리가 이 계정 암호를 변경할지 여부를 지정합니다.

참고: 배타적 계정이 아닌 경우 CA Access Control 엔터프라이즈 관리는 모든 사용자가 계정을 체크 인한 경우에만 새 권한 있는 계정 암호를 생성합니다.

"제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리가 새 권한 있는 계정을 만듭니다.

Break Glass 프로세스가 작동하는 방법

사용자가 관리 권한이 없는 계정에 즉시 액세스해야 하는 경우 Break Glass 체크 아웃을 수행합니다.

Break Glass 계정은 사용자 역할에 따라 사용자에게 할당되지 않은 권한 있는 계정입니다. 하지만 사용자는 필요한 경우 이 계정 암호를 획득할 수 있습니다.

Break Glass 체크 아웃 프로세스 중에 Break Glass 체크 아웃 프로세스가 발생했음을 알리는 알림 메시지가 역할 관리자에게 전달되지만 이 관리자는 이 프로세스를 승인 또는 중단시킬 수 없습니다.

체크 아웃된 Break Glass 계정은 "홈" 탭의 "Break Glass" 옵션에 있는 "내 체크 아웃한 권한 있는 계정" 탭에 추가됩니다.

참고: Break Glass 권한 있는 액세스 역할이 있는 사용자만 Break Glass 프로세스를 수행할 수 있습니다.

응용 프로그램 만들기

응용 프로그램을 만들면 PUPM 에이전트를 호출하는 스크립트를 실행하여 CA Access Control 끝점에서 권한 있는 계정을 가져오는 PUPM 에이전트를 사용할 수 있게 됩니다. 스크립트에서 하드 카피 암호를 PUPM 에이전트가 필요할 때만 가져오는 권한 있는 계정 암호로 바꿀 수 있습니다.

응용 프로그램은 CA Access Control 끝점에서 실행하는 스크립트를 나타냅니다.

사용할 모든 스크립트에 대해 하나의 응용 프로그램을 만들어 특정 권한 있는 계정을 이 스크립트에 할당합니다.

응용 프로그램을 만들려면

참고: 권한 있는 계정을 관리하려면 관리 권한이 있어야 합니다.

1. "권한 있는 계정", "응용 프로그램", "응용 프로그램 만들기"를 선택합니다.

   "응용 프로그램 만들기: 응용 프로그램 검색 화면"이 나타납니다.

2. 응용 프로그램 유형의 새 개체를 만들도록 선택한 다음 "확인"을 클릭합니다.

   "응용 프로그램 만들기" 창이 나타납니다.

3. 다음 세부 정보를 제공하여 양식을 완성합니다.

   이름

   응용 프로그램(스크립트)의 이름을 정의합니다.

   설명

   응용 프로그램(스크립트)에 대한 설명을 정의합니다.

   응용 프로그램 경로

   응용 프로그램(스크립트)의 전체 경로를 정의합니다.

   예: /opt/scripts/myscript/sh

   호스트

   스크립트를 실행할 대상 호스트의 이름을 정의합니다.

   예: myhost.com

   클라이언트 유형

   PUPM 에이전트의 유형을 지정합니다.

   옵션: CLI

   식별자 호스트

스크립트를 실행할 대상 호스트의 이름을 정의합니다.

예: myhost.com

식별자 사용자

스크립트를 실행하도록 허용된 사용자의 쉼표로 구분된 목록을 정의합니다.

예:mydomain/user1, mydomain/user2

계정

이 응용 프로그램과 관련된 권한 있는 계정을 정의합니다.

사용

이 응용 프로그램이 활성화되었는지 여부를 지정합니다.

4. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 응용 프로그램 설정을 만듭니다.

제 6 장: 권한 있는 계정 사용

이 장은 아래의 주제를 포함하고 있습니다.

권한 있는 계정 체크 아웃

계정이 속한 끝점을 관리하기 위해 권한 있는 계정을 체크 아웃합니다. 권한 있는 계정을 체크 아웃하면 CA Access Control 엔터프라이즈 관리는 관리되는 끝점에 액세스하기 위해 사용할 수 있는 암호를 표시합니다.

권한 있는 계정 암호를 체크 아웃하려면

1. "홈", "내 계정", "권한 있는 계정 체크 아웃" 탭을 차례로 선택합니다.

   "내 계정" 페이지가 열려 체크 아웃할 수 있는 계정을 표시합니다.

2. (선택 사항) 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 체크 아웃할 계정을 선택한 다음 "체크 아웃"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 작업을 제출하고 성공하는 경우 확인 메시지에 계정 암호를 표시합니다.

권한 있는 계정 체크 인

관리되는 끝점에서 로그아웃한 다음에는 권한 있는 계정을 체크 인합니다. 권한 있는 계정을 체크 인하면 CA Access Control 엔터프라이즈 관리가 암호를 변경할 수 있습니다(이렇게 설정된 경우).

권한 있는 계정을 체크 인하려면

1. "홈", "내 계정", "내 체크 아웃한 권한 있는 계정" 탭을 차례로 클릭합니다.

   "내 계정" 페이지가 열려 체크 인할 수 있는 계정을 표시합니다.

2. (선택 사항) 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 체크 인할 계정을 선택하고 "체크 인"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정을 체크 인합니다.

추가 정보:

권한 있는 계정 검색(페이지 118)
권한 있는 계정 체크 아웃(페이지 125)
권한 있는 계정에 대한 액세스 요청(페이지 126)

권한 있는 계정에 대한 액세스 요청

권한 있는 계정 암호가 필요하지만 자신의 사용자 계정에 이러한 계정을 체크 아웃할 수 있는 권한이 없는 경우 계정을 체크 아웃하기 위한 요청을 제출할 수 있습니다. CA Access Control 엔터프라이즈 관리는 요청을 승인 또는 거부할 수 있는 승인자에게 이 요청을 전달합니다. 승인되면 권한 있는 계정을 체크 아웃할 수 있습니다.

권한 있는 계정에 대한 암호를 요청하려면

1. "홈", "내 계정", "권한 있는 계정 요청"을 차례로 클릭합니다.

   "권한 있는 계정 요청: 권한 있는 계정 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 체크 아웃할 권한 있는 계정을 선택하고 "선택"을 클릭합니다.

4. 요청을 완성하고 "제출"을 클릭합니다.

   요청이 제출되었음을 알리는 창이 열립니다.

   요청이 승인자에게 전달되고 승인 또는 거부될 때까지 보류 상태로 유지됩니다. 요청이 승인되면 권한 있는 계정을 체크 아웃할 수 있습니다.

Break Glass

액세스 권한이 없는 끝점에 즉시 액세스해야 하는 경우 Break Glass 작업을 사용하십시오.

참고: 끝점에 즉시 액세스할 수 없는 경우 권한 있는 계정에 대한 액세스를 요청하고 요청이 승인될 때까지 기다릴 수 있습니다.

Break Glass 를 사용하려면

1. "홈", "내 계정", "Break Glass"를 클릭합니다.

   "Break Glass" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 체크 아웃할 권한 있는 계정을 선택하고 체크 아웃 이유를 입력한 다음 "체크 아웃"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 작업을 제출하고 성공하는 경우 확인 메시지에 계정 암호를 표시합니다.

Break Glass 권한 있는 계정 체크 인

관리되는 끝점에서 로그 아웃한 다음에는 Break Glass 권한 있는 계정을 체크 인합니다.

Break Glass 권한 있는 계정을 체크 인하려면

1. "홈", "내 계정", "Break Glass", "내 체크 아웃한 권한 있는 계정" 탭을 클릭합니다.

   "Break Glass" 페이지가 열려 체크 인할 수 있는 계정을 표시합니다.

2. (선택 사항) 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 체크 인할 계정을 선택하고 "체크 인"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정을 체크 인합니다.

권한 있는 계정의 강제 체크 인

하나 이상의 사용자에 의해 현재 체크 아웃된 권한 있는 계정을 강제 체크 인할 수 있습니다.

권한 있는 계정을 강제로 체크 인하려면

1. "권한 있는 계정", "계정", "강제 체크 인"을 클릭합니다.

   "강제 체크 인: 권한 있는 계정 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다. "사용자가 체크 아웃함" 열에서 권한 있는 계정의 체크 아웃 여부 및 체크 아웃한 사람에 대한 정보를 볼 수 있습니다.

3. 체크 인할 권한 있는 계정을 선택하고 "선택"을 클릭합니다.

   확인 메시지가 나타납니다.

4. 변경 사항을 승인하려면 "예"를 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정을 체크 인합니다.

권한 있는 계정 암호 자동 다시 설정

선택된 권한 있는 계정의 암호를 다시 설정하려면 자동 암호 다시 설정 작업을 사용하십시오. 초기화되었을 때 CA Access Control 엔터프라이즈 관리는 계정에 할당된 암호 정책을 기반으로 선택된 계정에 대한 새 암호를 생성합니다.

중요! 계정에 대한 암호를 다시 설정하면 이전 암호는 폐기됩니다. 이전 암호를 사용하는 모든 사용자가 계속 관리되는 장치에 로그인하려면 계정에 체크 인한 다음 체크 아웃해야 합니다.

참고: 이 옵션은 연결 해제된 계정에 대해 사용할 수 없습니다.

권한 있는 계정 암호를 자동으로 다시 설정하려면

1. "권한 있는 계정", "계정", "자동 계정 다시 설정"을 클릭합니다.

   "자동 계정 다시 설정: 권한 있는 계정 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 다시 설정할 권한 있는 계정을 선택하고 "선택"을 클릭합니다.

   확인 메시지가 나타납니다.

4. 변경 사항을 승인하려면 "예"를 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정 암호를 다시 설정합니다.

권한 있는 계정 암호 직접 다시 설정

계정 암호를 다시 설정하고 권한 있는 계정에 대한 새 암호를 직접 생성하려면 직접 암호 다시 설정 작업을 사용하십시오. 새 암호는 선택한 권한 있는 계정에 할당된 암호 정책을 준수해야 합니다.

중요! 계정에 대한 암호를 다시 설정하면 이전 암호는 폐기됩니다. 이전 암호를 사용하는 모든 사용자가 계속 관리되는 장치에 로그인하려면 계정에 체크 인한 다음 체크 아웃해야 합니다.

연결 해제된 끝점의 권한 있는 계정을 관리할 때만 직접 암호 다시 설정 기능을 사용하는 것이 좋습니다. 연결 해제된 끝점에서 암호를 변경할 때마다 CA Access Control 엔터프라이즈 관리가 저장하는 암호를 변경하십시오.

권한 있는 계정 암호를 직접 다시 설정하려면

1. "권한 있는 계정", "계정", "직접 암호 다시 설정"을 클릭합니다.

   "직접 암호 다시 설정: 권한 있는 계정 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 암호를 변경할 권한 있는 계정을 선택하고 "선택"을 클릭합니다.

   "직접 암호 다시 설정" 페이지가 나타납니다.

4. 새 암호를 입력하고 확인을 위해 다시 입력한 다음 "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정 암호를 변경합니다.

권한 있는 계정 요청에 응답

기본 PUPM 승인자 역할이 있거나 이에 준하는 역할이 할당된 경우 사용자들이 제출한 보류 중인 권한 있는 계정 액세스 요청에 응답할 수 있습니다. 다음 작업 중 하나를 사용하여 응답할 수 있습니다.

- **승인** - 요청을 승인하고 사용자가 권한 있는 계정을 체크 아웃할 수 있게 허용합니다.
- **거부** - 권한 있는 계정 요청을 거부합니다.
- **항목 예약** - 나중에 고려할 수 있도록 요청을 예약합니다. 요청을 예약하면 CA Access Control 엔터프라이즈 관리는 이 작업 항목을 다른 승인자의 작업 목록에서 제거합니다. 이 항목은 나중에 승인 또는 거부할 수 있습니다.
- **항목 해제** - 다른 승인자가 응답할 수 있도록 요청의 예약을 해제합니다. 이전에 자신이 예약했던 항목만 해제할 수 있습니다.

또한 다른 승인자를 추가하고 이 승인자들도 자신의 보류 중인 승인 목록에 작업 항목을 받을 수 있도록 해당 작업 항목을 다시 할당할 수도 있습니다.

참고: Break Glass 체크 아웃 요청은 요청의 "내 승인 대기" 목록에 표시됩니다. 하지만 이러한 요청을 승인 또는 거부할 필요는 없습니다. 이러한 요청은 사용자가 Break Glass 계정을 체크 아웃했음을 알리기 위해서만 표시됩니다.

참고: 권한 있는 계정 요청에 응답하려면 사용자에게 PUPM 승인자 권한 있는 액세스 역할이 있어야 하며 요청하는 사용자의 관리자여야 합니다.

권한 있는 계정 요청에 응답하려면

1. "홈", "내 계정", "내 승인 대기"를 클릭합니다.

   보류 중인 권한 있는 계정 요청의 목록이 나타납니다.

2. 고려할 보류 중인 요청을 클릭합니다.

   "권한 있는 계정 요청 승인" 페이지가 나타납니다.

3. (선택 사항) 이 요청에 대한 승인자를 추가하려면 다음 단계를 따릅니다.

   a. "할당받은 사람 추가"를 클릭합니다.

      "사용자 선택" 검색 창이 열립니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 사용자의 목록이 표시됩니다.

   c. 추가할 사용자를 선택하고 "선택"을 클릭합니다.

      사용자가 승인자 목록에 추가됩니다.

4. (선택 사항) 다음과 같이 요청 세부 내용을 검토하고 필요한 매개 변수를 수정합니다.
   a. "권한 있는 계정" 탭을 클릭합니다.

      "권한 있는 계정" 탭이 나타나고 이 안에 계정 및 요청의 세부 정보가 표시됩니다.

   b. "유효 날짜" 필드를 사용하여 체크 아웃 만료 시간을 다시 정의합니다.

   c. 이 요청에 대한 응답 설명을 입력합니다.
5. 다음 중 하나를 수행합니다.
   - "승인"을 클릭합니다.

     요청이 승인되어 보류 중인 요청 목록에서 제거되며, 이제 요청자가 권한 있는 계정을 체크 아웃할 수 있게 됩니다.
   - "거부"를 클릭합니다.

     해당 요청이 거부되고 보류 중인 요청 목록에서 제거됩니다.
   - "항목 예약"을 클릭합니다.

     요청이 예약되고 다른 승인자의 보류 중인 요청 목록에서 제거됩니다.
   - "항목 해제"를 클릭합니다.

     요청이 해제되고 다른 승인자가 사용할 수 있게 됩니다. 자신이 예약했던 항목만 해제할 수 있습니다.

권한 있는 계정 예외 삭제

권한 있는 계정 예외를 사용하면 사용자가 원래 체크 아웃할 수 있는 권한이 없는 계정을 체크 아웃할 수 있습니다. PUPM 승인자가 권한 있는 계정 액세스 요청을 승인하면 요청자는 요청이 유효한 기간 동안 권한 있는 계정을 체크 아웃할 수 있습니다. 예외가 적용되는 계정을 사용자가 체크 아웃하지 못하도록 방지하기 위해 권한 있는 계정 예외를 삭제할 수 있습니다. 권한 있는 계정 예외를 삭제하려면 사용하는 계정에 기본 권한 있는 계정 요청 또는 PUPM 대상 시스템 관리자 역할(또는 이 작업을 포함하는 동등한 역할)이 할당되어 있어야 합니다.

권한 있는 계정 요청을 삭제하려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "예외", "권한 있는 계정 예외 삭제"를 클릭합니다.

   "권한 있는 계정 예외 삭제: 권한 있는 계정 예외 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정 예외의 목록이 표시됩니다.

3. 삭제할 권한 있는 계정 예외를 선택하고 "선택"을 클릭합니다.

   선택한 권한 있는 계정 예외의 삭제를 확인하는 확인 메시지가 나타납니다.

4. "예"를 클릭합니다.

   권한 있는 계정 요청이 삭제됩니다.

제 7 장: 끝점에서 권한 있는 계정을 사용하여 작업

이 장은 아래의 주제를 포함하고 있습니다.

끝점에서 권한 있는 계정을 사용하여 작업하는 방법

CA Access Control 은 PUPM 에이전트를 사용하여 끝점에서 기본 PUPM 기능을 관리할 수 있게 해 줍니다. PUPM 에이전트는 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정에 대한 암호를 가져오기 위해 CA Access Control 엔터프라이즈 관리와 상호 작용합니다.

PUPM 에이전트는 끝점에서 CA Access Control 엔터프라이즈 관리에 정의된 권한 있는 계정에 대한 체크 아웃 및 체크 인 기능을 제공합니다.

또한 스크립트에서 PUPM 에이전트를 사용하여 스크립트에서 하드 코드된 암호를 대체할 수 있습니다. 스크립트가 실행될 때 PUPM 에이전트는 권한 있는 계정 자격 증명을 CA Access Control 엔터프라이즈 관리로 보냅니다. CA Access Control 엔터프라이즈 관리는 계정 설정을 검사하여 승인되는 경우 계정 암호를 반환합니다. 스크립트를 실행하여 권한 있는 계정 암호를 받을 수 있도록 허용되는 사용자의 목록을 정의할 수 있습니다.

참고: 스크립트에서 PUPM 을 사용하려면 CA Access Control 엔터프라이즈 관리에서 스크립트를 응용 프로그램으로 정의해야 합니다.

이 프로세스는 다음과 같이 작동합니다.

1. 다음 방법 중 하나로 PUPM 에이전트를 실행합니다.
   a. 명령 프롬프트 창에서 권한 있는 계정 암호를 체크 아웃 또는 체크 인합니다.
   b. 끝점에 있는 PUPM 에이전트를 호출하는 스크립트를 검토합니다.
2. PUPM 에이전트는 승인을 위해 요청을 CA Access Control 엔터프라이즈 관리에 전달합니다.

3. CA Access Control 엔터프라이즈 관리는 권한 있는 계정 암호를 끝점에 보내고 PUPM 에이전트는 암호를 표시하고 확인 메시지를 로깅합니다.
4. CA Access Control 엔터프라이즈 관리는 계정 암호를 다시 암호 저장소에 다시 체크 인하고 PUPM 에이전트는 확인 메시지를 로깅합니다.
5. PUPM 에이전트는 체크 인이 성공했음을 알리는 확인 메시지를 로깅합니다.

추가 정보:

응용 프로그램 만들기(페이지 123)

끝점에서 권한 있는 계정 암호 체크 아웃

권한 있는 계정 암호를 CA Access Control 끝점에서 직접 체크 아웃하려면 PUPM 에이전트를 사용하십시오. 그런 다음 이 암호를 사용하여 끝점에 있는 권한 있는 장치에 로그인할 수 있습니다.

끝점에서 권한 있는 계정 암호를 체크 아웃하려면 다음 명령을 입력하십시오.

```
acpwd -checkout -account name -ep name -eptype type [-container name] [-nologo]
```

계정 암호가 성공적으로 체크 아웃되었음을 알리는 확인 메시지가 나타납니다.

참고: 0(영)으로 표시된 확인 메시지는 성공적인 암호 체크 아웃을 나타냅니다. PUPM 에이전트 구문에 대한 자세한 내용은 참조 안내서를 참조하십시오.

끝점에서 권한 있는 계정 암호 체크 인

끝점에 있는 관리되는 장치에 로그인하기 위해 암호가 더 이상 필요 없는 경우에는 PUPM 에이전트를 사용하여 CA Access Control 끝점에서 권한 있는 계정 암호를 직접 체크 인하십시오.

끝점에서 권한 있는 계정 암호를 체크 인하려면 다음 명령을 입력하십시오.

```
acpwd -checkin -account name -ep name -eptype type [-container name] [-nologo]
```

계정 암호가 성공적으로 체크 인되었음을 알리는 확인 메시지가 나타납니다.

참고: 0(영)으로 표시된 확인 메시지는 성공적인 암호 체크 인을 나타냅니다. PUPM 에이전트 구문에 대한 자세한 내용은 참조 안내서를 참조하십시오.

하드 코드된 스크립트 암호를 체크 아웃된 권한 있는 계정 암호로 대체

스크립트 내에서 PUPM 에이전트를 사용하여 하드 코드된 암호를 CA Access Control 엔터프라이즈 관리에서 체크 아웃하는 암호로 대체할 수 있습니다. 이렇게 하면 하드 코드된 암호를 스크립트 내에 포함해야 할 필요가 없게 됩니다.

참고: 스크립트에서 PUPM 을 사용하려면 CA Access Control 엔터프라이즈 관리에서 스크립트를 응용 프로그램으로 정의해야 합니다.

하드 코드된 스크립트 암호를 체크 아웃한 권한 있는 계정 암호로 대체하려면 스크립트에 다음 명령을 추가하십시오.

```
acpwd -checkout -account name -ep name -eptype type [-container name] -nologo
```

또한 명령의 출력(체크 아웃한 권한 있는 계정 암호)을 사용하도록 스크립트를 수정해야 합니다.

참고: PUPM 에이전트 구문에 대한 자세한 내용은 참조 안내서를 참조하십시오.

예: Windows 에 설치된 PUPM 에이전트를 사용하여 권한 있는 계정 암호를 체크 아웃하는 스크립트

다음은 Windows 에서 권한 있는 계정 암호를 체크 아웃하기 위해 PUPM 에이전트를 호출하는 예제 스크립트의 내용입니다. 이 예제는 PUPM 에이전트가 CA Access Control 끝점에 설치되어 있고 CA Access Control 엔터프라이즈 관리에서 응용 프로그램을 정의했다고 가정합니다.

이 예제의 스크립트는 CA Access Control 엔터프라이즈 관리에서 가져오는 권한 있는 계정 암호를 사용하여 Windows 레지스트리에서 항목을 추가 및 삭제합니다.

```
set AdminUser=PowerUser
FOR /F "tokens=*" %%i IN ('"C:\Program Files\AccessControl\bin\acpwd.exe" -checkout
-account PowerUser -ep comp1_123 -eptype "Windows Agentless" -container "Windows
Accounts" -nologo') DO SET AdminPassword=%%i
set runasadmin="C:\utils\psexec.exe" -u %AdminUser% -p
%runasadmin% %AdminPassword% REG ADD "HKLM\SOFTWARE\PUPM Registry"
%runasadmin% %AdminPassword% REG DELETE "HKLM\SOFTWARE\PUPM Registry" /F
```

이 예에서 스크립트는 PUPM 에이전트를 실행하여 권한 있는 계정 암호를 체크 아웃합니다. 이 스크립트는 계정 이름(PowerUser), 끝점 이름(comp1_123), 끝점 유형(Windows Agentless), 사용자의 컨테이너 이름(Windows Accounts)을 포함하고 있습니다. 이 스크립트는 PUPM 에이전트가 암호만 표시하도록 지시하고, 이 암호를 사용하여 레지스트리 항목을 추가 및 삭제하기 위한 관리 사용자로서 PsExec 프로그램을 실행하기 위해 이 암호를 사용합니다.

추가 정보:

응용 프로그램 만들기(페이지 123)

제 8 장: UNAB 사용

이 장은 아래의 주제를 포함하고 있습니다.

UNAB 구성 요소

UNIX 인증 브로커(UNAB)는 Active Directory 사용자의 UNIX 호스트에 대한 액세스를 관리하고 제어하는 여러 구성 요소로 구성되어 있습니다.

- **UNAB 인증 에이전트** - UNAB 인증 에이전트(uxagent) 데몬은 Active Directory 와 연결하고 사용자 인증, 권한 부여, Active Directory 에 사용자 등록, 사용자/그룹 마이그레이션, 로컬 액세스 파일 관리 등과 관련하여 Active Directory 연결의 보안을 유지할 책임이 있습니다.
- **uxconsole** - uxconsole 은 UNIX 호스트를 Active Directory 에 등록하고, 사용자/그룹을 마이그레이션하고, UNAB 를 활성화하는 데 사용하는 UNAB 관리 콘솔입니다. uxconsole 을 사용하여 UNAB 가 설치된 모든 UNIX 호스트에서 로그인하는 사용자를 관리할 수 있습니다.
- **CA Access Control 엔터프라이즈 관리 UNAB** - CA Access Control 엔터프라이즈 관리는 중앙 위치에서 UNAB 호스트를 관리할 수 있게 해 줍니다. CA Access Control 엔터프라이즈 관리를 사용하면 회사 내의 모든 UNAB 호스트에 대한 Active Directory 사용자 및 그룹의 액세스를 제어할 수 있습니다.

UNAB 설정 방법

UNIX 인증 브로커(UNAB)가 UNIX 호스트에 대한 액세스를 제어하는 방식을 이해하면 구현 및 구성 프로세스 중에 도움이 됩니다.

UNIX 호스트에서 UNAB 를 설치한 이후에 UNAB 를 Active Directory 에 등록하고 UNAB 를 활성화하여 엔터프라이즈 사용자 로그인 인증을 활성화합니다. 그런 다음에 마이그레이션 프로세스를 시작하여 로컬 사용자와 그룹을 Active Directory 로 마이그레이션할 수 있습니다.

1. UNAB 가 설치되면 UNIX 호스트를 Active Directory 에 등록합니다.

   이 단계에서 UNAB 는 어떠한 로그인 요청도 차단하지 않습니다.

2. UNIX 호스트에 대한 액세스를 허용 또는 거부할 엔터프라이즈 사용자 및 그룹을 정의합니다. 이 작업은 CA Access Control 엔터프라이즈 관리에서 로그인 권한 부여 정책을 만들어 수행할 수 있습니다.
3. UNAB 를 활성화하여 UNIX 호스트에 대한 엔터프라이즈 사용자 인증을 활성화합니다.
4. 새 사용자가 로그인할 수 있게 하려면 추가 엔터프라이즈 사용자 및 그룹을 UNAB 로그인 권한 부여 정책에 추가합니다.

   이 단계에서 로컬 사용자 저장소(예: etc.passed) 또는 UNAB 로그인 권한 부여 정책에 정의된 사용자에 대해 로그인이 허용됩니다.

5. UNAB 가 활성화된 이후에 사용자 및 그룹을 Active Directory 로 마이그레이션할 수 있게 됩니다.

UNAB 가 사용자를 인증하는 방법

UNIX 호스트에서 UNAB 를 설치하여 구성한 다음에는 선택한 통합 모드에 따라 사용자가 자신의 Active Directory 사용자 계정이나 로컬 사용자 계정을 사용하여 로그인할 수 있게 됩니다.

사용자가 UNAB 가 실행 중인 UNIX 호스트에 로그인하려고 시도하면 다음이 발생합니다.

1. 사용자가 유효한 Active Directory 또는 로컬 계정 사용자 이름 및 암호를 입력하도록 요청을 받습니다.
2. UNAB 가 Active Directory, 로그인 인증 정책, 로컬 호스트 액세스 파일을 사용하여 사용자의 자격 증명을 인증하고 사용자 계정에서 가져온 추가 정보를 검사합니다.
3. 사용자가 인증되면 UNAB 는 UNIX 호스트에 사용자가 액세스할 수 있도록 허용합니다. 그렇지 않은 경우 UNAB 는 호스트에 대한 사용자의 액세스를 차단합니다.

호스트 액세스를 제어하고 UNAB 를 구성하는 방법

CA Access Control 엔터프라이즈 관리를 통해 UNIX 호스트에 대한 사용자 및 그룹 액세스를 제어하고 UNAB 호스트를 구성할 수 있습니다. 특정 사용자 및 그룹에게만 호스트에 대한 로그인을 허용하는 액세스 권한을 부여하여 UNIX 호스트에 대한 사용자 및 그룹 액세스를 제어합니다.

호스트에 대한 액세스를 제어하는 것과 동일한 방법으로 UNAB 호스트를 구성합니다. CA Access Control 엔터프라이즈 관리를 사용하여 회사 내 UNAB 호스트의 기능을 먼저 제어한 다음 다른 모든 호스트에 적용합니다.

사용자 및 그룹을 할당하거나 토큰 값을 정의하면 CA Access Control 엔터프라이즈 관리는 이 정보를 정책에 적용하고 다음을 수행합니다.

1. CA Access Control 엔터프라이즈 관리는 사용자 및 그룹의 목록을 포함하거나 구성 매개 변수를 포함하는 배포 패키지를 만들어 정책을 적용할 호스트 또는 호스트 그룹에 할당합니다.
2. CA Access Control 엔터프라이즈 관리는 호스트에 배포하기 위해 이 패키지를 배포 서버에 전달합니다.
3. UNAB 는 배포 서버에서 이 패키지를 가져와 정책을 설치한 다음 CA Access Control 엔터프라이즈 관리에 확인 메시지를 보냅니다.

참고: 호스트에 엔터프라이즈 정책과 UNAB 로그인 정책을 모두 배포한 경우 엔터프라이즈 정책이 UNAB 로그인 정책보다 우선 순위가 높습니다.

UNAB 로그인 권한 부여 관리

UNAB 호스트 또는 호스트 그룹에 대한 사용자의 로그인을 제어하려면 액세스 권한을 부여할 사용자 또는 그룹의 목록을 만듭니다. 이 목록은 CA Access Control 엔터프라이즈 관리가 선택된 호스트 또는 호스트 그룹에 할당 및 배포하는 정책에 작성됩니다. 로그인 정책의 이름은 login@hostName 으로 설정됩니다.

참고: "배포 감사" 작업을 사용하여 정책의 배포 상태를 볼 수 있습니다.

UNAB 로그인 권한 부여를 관리하려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "정책 관리"를 클릭합니다.
   b. "UNIX 인증" 하위 탭을 클릭합니다.

      사용 가능한 작업 목록이 나타납니다.

2. 다음 작업 중 하나를 수행합니다.
   - "호스트 로그인 권한 부여 관리"를 클릭합니다.

     "호스트 로그인 권한 부여 관리: 호스트 검색" 화면이 나타납니다.
   - "호스트 그룹 로그인 권한 부여 관리"를 클릭합니다.

     "호스트 그룹 로그인 권한 부여 관리: 호스트 그룹 검색" 화면이 나타납니다.
3. 수정할 호스트 또는 호스트 그룹의 이름을 입력하고 "검색"을 클릭합니다.

   필터 조건과 일치하는 호스트 또는 호스트 그룹의 목록이 나타납니다.
4. 수정할 호스트 또는 호스트 그룹을 선택하고 "선택"을 클릭합니다.

   "호스트 로그인 권한 부여 관리: HostName" 또는 "호스트 그룹 로그인 권한 부여 관리: HostGroupName" 페이지가 나타납니다.
5. (선택 사항) 다음과 같이 사용자를 추가합니다.
   a. "사용자 추가"를 클릭합니다.

      "사용자 선택" 페이지가 나타납니다.
   b. 검색 매개 변수를 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 사용자의 목록이 표시됩니다.
   c. 액세스 권한을 부여할 사용자를 선택한 다음 "선택"을 클릭합니다.

      선택한 사용자가 권한이 부여된 사용자 및 그룹 목록에 나타납니다.
6. (선택 사항) 다음과 같이 그룹을 추가합니다.
   a. 그룹 추가를 클릭합니다.

      "그룹 선택" 페이지가 나타납니다.
   b. 검색 매개 변수를 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 그룹의 목록이 표시됩니다.
   c. 액세스 권한을 부여할 그룹을 선택한 다음 "선택"을 클릭합니다.

      선택한 그룹이 권한이 부여된 사용자 및 그룹 목록에 나타납니다.
7. (선택 사항) 다음과 같이 사용자 및 그룹을 제거합니다.
   a. 권한이 부여된 사용자 및 그룹 목록에서 제거할 사용자 및 그룹을 선택합니다.
   b. "제거"를 클릭합니다.

      선택한 사용자 및 그룹은 권한이 부여된 사용자 및 그룹 목록에서 제거됩니다.

8. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 사용자 및 그룹의 업데이트된 목록을 지정된 호스트 또는 호스트 그룹에 할당합니다.

UNAB 호스트 또는 호스트 그룹 구성

UNAB 호스트 및 호스트 그룹을 제어하는 구성 설정을 정의할 수 있습니다. CA Access Control 엔터프라이즈 관리는 UNAB 구성 파일(uxauth.ini) 또는 CA Access Control 구성 파일(accommon.ini)의 설정 값을 설정하는 데 도움을 줍니다. 구성 설정에 값을 할당하면 CA Access Control 엔터프라이즈 관리는 업데이트된 설정 값을 포함하는 구성 정책을 만들어 호스트 또는 호스트 그룹에 할당합니다. 정책 이름은 config@hostName 으로 설정됩니다.

참고: "배포 감사" 작업을 사용하여 정책의 배포 상태를 볼 수 있습니다.

UNAB 호스트 또는 호스트 그룹을 구성하려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "정책 관리"를 클릭합니다.
   b. "UNIX 인증" 하위 탭을 클릭합니다.

      사용 가능한 작업 목록이 나타납니다.
2. 다음 작업 중 하나를 수행합니다.
   - "UNAB 호스트 구성"을 클릭합니다.

     "UNAB 호스트 구성: 호스트 검색" 화면이 나타납니다.
   - "UNAB 호스트 그룹 구성"을 클릭합니다.

     "UNAB 호스트 그룹 구성: 호스트 그룹 검색" 화면이 나타납니다.
3. 수정할 호스트 또는 호스트 그룹의 이름을 입력하고 "검색"을 클릭합니다.

   필터 조건과 일치하는 호스트 또는 호스트 그룹의 목록이 나타납니다.
4. 수정할 호스트 또는 호스트 그룹을 선택하고 "선택"을 클릭합니다.

   "UNAB 구성: HostName" 또는 "UNAB 구성: HostGroupName" 화면이 나타납니다.
5. 수정할 섹션 및 토큰을 선택하고 "토큰 추가"를 클릭합니다.

   지정된 구성 토큰이 나타납니다.
6. 구성 토큰의 값을 수정합니다.

   참고: 구성 토큰에 대한 자세한 내용은 참조 안내서를 참조하십시오.

7. (선택 사항) 수정할 다른 섹션 및 토큰을 선택하고, "토큰 추가"를 클릭하고, 구성 토큰의 값을 필요한 대로 수정합니다.
8. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 선택한 UNAB 호스트 및 호스트 그룹의 구성 토큰 값을 설정합니다.

CA Access Control 엔터프라이즈 관리가 호스트에 정책을 커밋했는지 확인

권한 부여 및 구성 목록을 작성한 다음에는 CA Access Control 엔터프라이즈 관리가 변경 내용을 UNAB 호스트의 배포 감사 옵션에 커밋했는지 확인할 수 있습니다.

CA Access Control 엔터프라이즈 관리가 호스트에 정책을 커밋했는지 확인하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리" 탭, "정책" 작업을 차례로 선택한 다음 "배포" 옵션을 확장합니다.

   배포 옵션 메뉴가 열립니다.
2. "배포 감사" 옵션을 선택합니다.

   배포 감사 검색 화면이 열립니다.
3. 표시할 호스트 및 정책을 선택하고 "실행"을 클릭합니다.

   쿼리에 대한 검색 결과가 표시됩니다.

   참고: 로그인 정책의 이름은 **login@**으로 시작됩니다.
4. 결과 줄을 클릭하여 배포 상태를 표시합니다.

   CA Access Control 엔터프라이즈 관리는 배포 작업의 상태 및 출력을 표시합니다.

마이그레이션 충돌 해결

UNAB 는 마이그레이션 프로세스 중에 발견한 충돌을 충돌 파일에 로깅합니다. 이 파일은 로컬 호스트에서 Active Directory 로 사용자 및 그룹을 마이그레이션하지 못하게 만든 충돌의 원인에 대한 자세한 정보를 수록합니다.

이 충돌 파일을 CSV 파일로 내보내 컴퓨터로 다운한 다음 검토하여 충돌을 해결할 수 있습니다. 나중에 수정된 스프레드시트를 CA Access Control 엔터프라이즈 관리로 다시 업로드하면 메시지 큐 서버로 이 시트가 전달됩니다. UNAB 는 이 파일을 검색한 다음 마이그레이션 프로세스를 다시 시작하여 이전에 마이그레이션되지 않은 사용자 및 그룹을 마이그레이션합니다.

참고: 호스트 그룹을 마이그레이션하는 경우 충돌 파일을 다운로드할 수 없습니다. 하지만 마이그레이션 프로세스의 충돌을 해결할 수 있도록 수정된 충돌 파일을 업로드할 수 있습니다.

마이그레이션 충돌을 해결하려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "정책 관리"를 클릭합니다.
   b. "UNIX 인증" 하위 탭을 클릭합니다.

      사용 가능한 작업 목록이 나타납니다.
2. 다음 작업 중 하나를 수행합니다.
   - "호스트 마이그레이션 충돌 해결"을 클릭합니다.

     "호스트 마이그레이션 충돌 해결: 호스트 검색" 화면이 나타납니다.
   - "호스트 그룹 마이그레이션 충돌 해결"을 클릭합니다.

     "호스트 그룹 마이그레이션 충돌 해결: 호스트 그룹 검색" 화면이 나타납니다.
3. 충돌을 해결할 호스트 또는 호스트 그룹의 이름을 입력한 다음 "검색"을 클릭합니다.

   필터 조건과 일치하는 호스트 또는 호스트 그룹의 목록이 나타납니다.
4. 충돌을 해결할 호스트 또는 호스트 그룹을 선택한 다음 "선택"을 클릭합니다.

   "UNAB 마이그레이션: HostName" 또는 "UNAB 마이그레이션: HostGroupName" 페이지가 나타납니다.

5. (선택 사항) 다음과 같이 호스트 마이그레이션에 대한 충돌 파일을 다운로드한 다음 충돌을 해결합니다.

   a. "UNAB 마이그레이션 충돌 세부 정보 다운로드" 섹션에 있는 "내보내기 및 다운로드" 링크를 선택합니다.

      대화 상자 창이 열립니다.

   b. 파일을 저장할 위치로 이동한 다음 "저장"을 선택합니다.

      CSV 파일이 지정된 위치로 다운로드됩니다.

   c. 이 CSV 파일을 열고 보고된 충돌을 해결한 다음 저장하고 파일을 닫습니다.

6. (선택 사항) 호스트 그룹 마이그레이션에 대한 충돌을 해결하는 CSV 파일을 만들어 저장합니다.

7. 다음과 같이 호스트 및 호스트 그룹 마이그레이션에 대한 충돌을 해결하는 CSV 파일을 업로드합니다.

   a. "UNAB 마이그레이션 솔루션 업로드" 섹션에서 "찾아보기" 단추를 선택합니다.

      대화 상자 창이 열립니다.

   b. 파일을 찾은 다음 "열기"를 클릭합니다.

   c. "업로드"를 클릭합니다.

      파일이 업로드됩니다.

8. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 파일을 메시지 큐 서버로 보냅니다. UNAB 는 큐에서 파일을 검색하고 마이그레이션 프로세스를 다시 시작하여 해결된 계정과 그룹의 마이그레이션을 시도합니다.

9. 마이그레이션이 끝난 후 충돌 파일을 다시 검토하여 이전에 충돌 파일에서 보고된 사용자 및 그룹이 성공적으로 마이그레이션되었는지 확인합니다.

예: UNAB 충돌 파일 출력

다음 예는 마이그레이션 프로세스 중 작성된 UNAB 충돌 파일의 출력 내용입니다.

```
USER,john,MIGRATE,,NO AD,1354,/tmp,201,,,user for doall proc
```

이 예에서 UNAB 는 사용자 john 이 Active Directory 로 마이그레이션(MIGRATE)되었고 충돌이 발견되지 않았음(NO)을 보고했습니다. 또한 이 파일에는 사용자 ID(1354), 홈 디렉터리(/tmp), 그룹 ID(201), GECOS 정보(user for doall proc)가 표시되어 있습니다.

참고: UNAB 충돌 파일에 대한 자세한 내용은 참조 안내서를 참조하십시오.

UNAB 중지

Active Directory 사용자가 UNIX 컴퓨터에 액세스할 수 없도록 하거나 UNAB 의 새 버전을 설치하려는 경우 UNAB 를 중지해야 합니다.

uxauthd 데몬을 중지하여 UNAB 를 중지합니다.

UNAB 를 중지하려면

1. superuser 로 UNIX 컴퓨터에 로그인합니다.
2. 다음 명령을 입력합니다.

   ```
   ./uxauthd -stop
   ```

   UNAB 데몬이 중지됩니다.

   데몬이 중지되었음을 알리는 메시지가 표시됩니다.

UNAB 상태 보기

UNAB 의 최신 상태를 보려면 이 옵션을 사용하십시오.

UNAB 상태를 보려면

1. 해당 컴퓨터의 관리 권한이 있는 사용자로 UNIX 컴퓨터에 로그인합니다.
2. 다음 인수를 사용하여 uxauthd 프로그램을 실행합니다.

   ```
   ./uxauthd -status
   ```

   UNAB 의 현재 상태를 알리는 메시지가 표시됩니다.

UNAB 디버그 파일

uxauth.ini 파일에 있는 UNAB 구성 파일의 에이전트 섹션은 런타임에 에이전트에 의해 수집된 디버깅 정보를 정의합니다. 기본적으로 UNAB 는 다음 파일에 디버그 정보를 수집합니다.

<install dir>/log/debug/

/gent_debug

디버그 메커니즘이 UNAB 디버그 파일에서 활성화되어 있는 한, 에이전트는 시작(시작 옵션 사용)할 때 디버그 파일에 디버그 메시지를 로깅합니다.

-debug 옵션을 사용하여 UNAB 를 시작하는 경우 디버그 메시지가 사용자 콘솔에 나타납니다.

제 9 장: 보고서 작성

이 장은 아래의 주제를 포함하고 있습니다.

보안 표준

여러 기업들이 문서 기반 작업 환경에서 전자 미디어 중심의 작업 환경으로 마이그레이션하는 과정에서 관련 데이터에 대한 로컬 및 원격 공격에 더욱 많이 노출되고 있습니다. 이러한 문제를 해결하기 위해 일반적인 전역 보안, 재무 정확도 및 보고, 개인 금융 정보 및 개별 ID 의 안전한 보호, 의료 관련 정보 보호, 미국 정부 차원의 보안 모범 사례 표준화 등 여러 영역에서 몇몇 보안 이니셔티브가 구현되었습니다.

아래의 보안 표준, 법령 및 요구 사항은 CA Access Control 보고 서비스에서 실행되고 있는 모범 사례 보고의 본질적인 내용을 효과적으로 요약해서 설명합니다.

PCI DSS(Payment Card Industry Data Security Standards)

PCI DSS 는 사기 및 해킹을 비롯한 보안 문제를 방지하기 위해 주요 신용 카드 회사에서 개발한 업계 표준입니다. 신용 카드 및 직불 카드 데이터를 수락, 캡처, 저장, 전송 또는 처리하는 회사는 PCI DSS 를 준수해야 합니다.

HIPAA(Health Insurance Portability and Accountability Act)

HIPAA 는 근로자가 이직하거나 실직하는 경우에도 건강 보험을 적용받을 수 있게 해주는 미국 연방법입니다. HIPAA 는 또한 보건 데이터의 보안 및 개인 정보 보호 문제를 다룹니다.

SOX(Sarbanes-Oxley Act)

SOX 는 재무 보고 표준을 규정하는 미국 연방법입니다. 이 법은 모든 미국 공개된 회사의 이사회 및 경영진에 적용됩니다.

보고서 유형

두 가지 다른 보고서 유형으로 CA Access Control 데이터 및 이벤트에 대한 정보를 볼 수 있습니다.

- CA Access Control 보고서 - 누가 무엇을 할 수 있는지 설명합니다.

  CA Access Control 보고서는 각 끝점에 있는 CA Access Control 데이터베이스의 데이터에 대한 정보(끝점 및 정책 위반에 배포하는 규칙 및 정책)를 제공합니다. CA Access Control 보고서는 CA Business Intelligence 에서 볼 수 있습니다.

- 감사 보고서 - 누가 무엇을 했는지 설명합니다.

  감사 보고서는 각 끝점에 있는 감사 로그 파일(seos.audit)의 데이터에 대한 정보(어떤 사용자가 끝점에서 어떤 작업을 수행했는지에 대한 정보)를 제공합니다. 감사 보고서는 CA Enterprise Log Manager 및 CA Access Control 엔터프라이즈 관리에서 볼 수 있습니다.

  참고: CA Enterprise Log Manager 에서 감사 보고서를 보는 방법에 대한 자세한 내용은 CA Enterprise Log Manager Overview Guide(CA Enterprise Log Manager 개요 안내서)를 참조하십시오.

참고: CA Access Control 보고서와 CA Access Control 감사 보고서를 보려면 추가 구성 요소를 설치하여 구성해야 합니다. 자세한 내용은 구현 안내서를 참조하십시오.

보고 서비스

CA Access Control 보고 서비스를 사용하면 한 위치에서 각 끝점(사용자, 그룹 및 리소스)의 보안 상태를 볼 수 있습니다. 예약을 통해 또는 요청 시에 각 끝점에서 데이터를 수집할 수 있습니다. 어떤 사용자가 어떤 리소스에 액세스할 수 있는 권한이 있는지 확인하기 위해 각 끝점에 일일이 연결할 필요가 없습니다. CA Access Control 보고 서비스는 한 번 설치되면 각 끝점에서 데이터를 수집하여 중앙 서버에 보고하기 위해 독립적으로 작동하며 사용자가 수동 작업을 할 필요 없이 끝점 상태를 계속 보고합니다. 즉 수집 서버가 가동되고 있는지 또는 중지되었는지에 관계없이 각 끝점에서 해당 상태를 보고합니다.

CA Access Control 보고 서비스는 BS 7799/ISO 17799, SOX(Sarbanes-Oxley), PCI(Payment Card Industry), HIPAA(Health Insurance Portability and Accountability Act), FISMA(Federal Information Security Management Act) 환경 등에 유용하며 수천 개의 끝점에서 사용자, 그룹 및 리소스 액세스의 실제 끝점 상태를 확인해야 하는 모든 경우에 도움이 됩니다.

보고 서비스는 각 끝점에서 수집한 데이터를 검색할 수 있도록 구성되어 있습니다. 다양한 용도에 맞게 사용자 지정 보고서를 작성하거나 CA Access Control 에서 기본적으로 제공하는 기존 보고서를 사용할 수 있습니다. 보고 서비스는 서버를 기반으로 하므로, 이 서비스를 사용하면 한 곳에서 보고서를 저장하고 관리할 수 있으며 보고서에 안전하게 액세스(SSL)할 수 있습니다. 항상 사용 가능하도록 보고 서비스를 구성할 수 있습니다. 단일 서버나 분산 구성에서 보고 서비스 구성 요소를 설치할 수 있습니다.

참고: 보고 서비스 구성 요소는 CA Access Control 적용 시스템 외부에서 작동하므로, 기존 구현을 다시 구성할 필요 없이 효율적으로 사용할 수 있습니다.

보고 서비스 구성 요소

보고 서비스는 다음 핵심 구성 요소로 구성됩니다.

- 보고서 에이전트는 각각의 CA Access Control 또는 UNAB 에서 실행되는 Windows 서비스 또는 UNIX 데몬이며, 배포 서버에 있는 구성된 메시지 큐의 큐로 정보를 보냅니다.
- 메시지 큐는 보고서 에이전트가 보내는 끝점 정보를 받기 위해 구성된 배포 서버의 구성 요소입니다. 보고를 위해 메시지 큐는 CA Access Control 웹 서비스를 사용하여 중앙 데이터베이스에 전달합니다. 중복 및 장애 조치를 위해 정보를 수집하고 전달하는 여러 개의 보고서 서버를 사용할 수 있습니다.
- 중앙 데이터베이스는 보고를 포함한 CA Access Control 엔터프라이즈 관리의 기능에 대한 정보를 수록하는 관계형 데이터베이스 관리 시스템(RDBMS)입니다. 다양한 도구를 사용하여 데이터베이스에 저장된 데이터에서 CA Access Control 구현에 대한 정보를 검색할 수 있습니다.
- 보고서 포털은 CA Access Control 보고서를 제공하는 응용 프로그램 서버입니다. 이 서버는 BusinessObjects InfoView 포털을 사용하므로 사용자가 중앙 데이터베이스에 저장된 보고 정보를 활용할 수 있습니다.
- 일반적인 보고 시나리오의 경우 데이터를 쉽게 작성할 수 있도록 기본 제공 보고서가 포함되어 있습니다.
- 보고서를 확인하고 관리할 수 있는 웹 기반 인터페이스를 실행하는 컴퓨터입니다.

참고: CA Access Control 보고 서비스 구현 및 아키텍처에 대한 자세한 내용은 구현 안내서를 참조하십시오.

보고 서비스 작동 방법

보고 서비스를 사용하면 각 끝점에서 수집된 데이터를 검색할 수 있습니다. 보고 서비스를 제대로 설정하려면 보고 서비스가 어떤 방식으로 데이터를 수집 및 저장하고 해당 데이터에서 보고서를 생성하는지 알아야 합니다.

보고 서비스는 다음 작업을 수행합니다.

- 각 끝점에서 데이터를 수집합니다.
- 이 데이터를 중앙 서버에 저장합니다.
- 저장된 데이터에서 보고서를 생성합니다.

  중앙 데이터베이스에 사용 가능한 데이터가 있으면 보고서 포털(BusinessObjects InfoView 포털의 CA 버전으로, 중앙 데이터베이스에 연결하도록 구성되고 바로 사용 가능한 CA Access Control 보고서가 함께 제공됨)을 사용하여 보고서를 생성하고 저장된 데이터를 검색할 수 있습니다.

각 끝점에서 보고용 데이터를 수집하는 방법

보고서를 생성하려면 각 끝점에서 데이터를 수집해야 합니다. 보고 서비스는 각 끝점에 설치된 보고서 에이전트를 사용하여 예약된 시간에 또는 요청 시 해당 끝점에서 데이터를 수집합니다.

참고: 보고서 에이전트는 CA Enterprise Log Manager 와의 통합에 대한 감사 데이터를 수집하고 라우팅하는 역할도 수행합니다. 이 프로세스에서는 보고서 에이전트가 끝점에 대한 보고를 위해 수행하는 작업만 설명합니다.

보고서 에이전트는 각 끝점에서 다음 작업을 수행합니다.

1. 위반 계산을 수행하고 그 결과를 배포 서버로 보냅니다.

   중요! 보고서 에이전트를 정기적으로 실행하도록 설정하고 DMS 를 업데이트할 필요가 없는 경우에는 정책 위반 계산을 별도로 예약할 필요가 없습니다.

2. 끝점에서 CA Access Control 데이터베이스(seosdb)와 각 PMDB(정책 모델 데이터베이스)의 복사본을 작성합니다.

   이 복사본은 CA Access Control 성능에 영향을 미치지 않고 데이터를 처리할 수 있도록 보고서 에이전트가 사용하는 임시 복사본입니다.

3. 각 데이터베이스에서 XML 구조로 데이터를 덤프합니다.

   이 덤프는 데이터베이스에 있는 모든 개체의 덤프입니다. 즉, selang 같은 데이터베이스 인터페이스 유틸리티를 통해 표시되는 데이터뿐만 아니라 모든 데이터가 캡처됩니다.

4. 데이터베이스의 XML 버전을 배포 서버로 보냅니다.

   보고서 에이전트는 데이터를 배포 서버의 보고 큐로 보냅니다.

각 끝점의 데이터를 처리 및 저장하는 방법

각 끝점에서 수집된 데이터는 처리를 위해 배포 서버로 보내집니다. 처리된 데이터는 보고서 생성을 위해 중앙 데이터베이스에 전송되어 저장됩니다.

배포 서버에서는 다음 작업을 수행합니다.

1. 끝점의 보고서 에이전트로부터 전체 데이터베이스의 스냅샷인 XML 덤프를 받습니다.

   각 XML 덤프는 전체 데이터베이스의 스냅샷입니다.

2. 데이터베이스 스키마에 따라 MDB(Message Driven Bean)를 사용하여 XML 덤프를 처리합니다.

   들어오는 각 XML 메시지 파일은 중앙 데이터베이스에 배치할 수 있도록 Java 개체로 변환됩니다.

3. 각 Java 개체는 중앙 데이터베이스에 삽입됩니다.

   이제 중앙 데이터베이스에서 끝점의 데이터를 검색할 수 있습니다.

표준 보고서

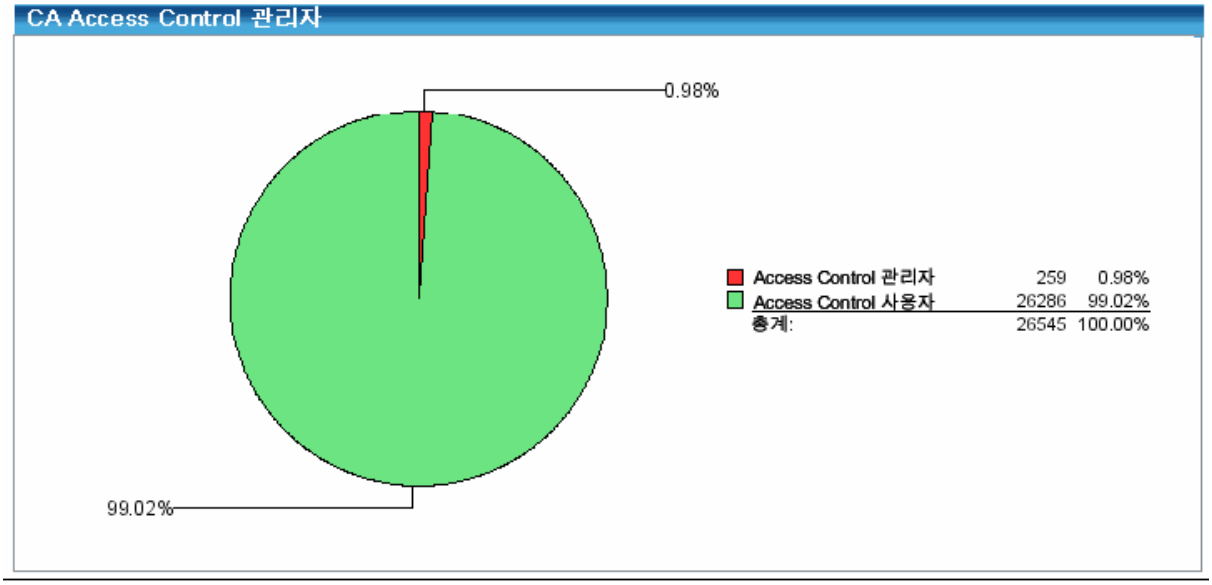
기본적으로 CA Access Control 보고 서비스는 기본 제품 설치의 일부로 표준 보고서와 함께 제공됩니다. 보고서는 다음과 같은 범주로 구분되어 있습니다.

- 계정 관리 보고서(페이지 154)
- 권한 보고서(페이지 158)
- 기타 보고서(페이지 160)
- 정책 관리 보고서(페이지 162)
- 암호 정책 보고서(페이지 166)
- 권한 있는 계정 관리 보고서(페이지 167)
- UNIX 인증 브로커 보고서(페이지 171)

표준 보고서 이외에도 보고서를 확장하고 다른 기능이 포함된 비슷한 보고서를 만들거나 완전히 새로운 보고서를 생성할 수 있습니다.

보고서 모양

보고서 출력에는 필요에 따라 표와 그래픽이 적절하게 사용됩니다. 예를 들어 간편하게 참조하여 특정 끝점 위치의 취약점을 한눈에 확인할 수 있도록 파이형 차트 그래픽이 제공됩니다. 아래 그림과 같이 CA Access Control 관리자 보고서에는 CA Access Control 관리자 역할을 수행하는 끝점 사용자의 수를 나타내는 파이형 차트가 제공됩니다. 일반 사용자에 비해 관리자의 비율이 높으면 보안상 위험할 수 있으므로 그래픽을 통해 보안 노출이 있는지 여부를 신속하게 알 수 있습니다. 이 예제 차트에서 커다란 빨간색 쐐기 모양은 현재 엔터프라이즈 사용자 기반의 거의 1%가 CA Access Control 관리를 수행할 수 있음을 나타내기 때문에 보안상 위험하다는 것을 나타냅니다.



그래픽 이외에도 각 보고서에는 실제 끝점 값에 대해 연관된 목록이 있습니다. 다음은 CA Access Control 관리자 보고서에서 가져온 이 표의 샘플입니다.

CA Access Control 관리자

사용자 이름	전체 이름	호스트 ID	관리자 모드 사용	암호 관리자 모드 사용	운영자 모드 사용
_seagent					
		SYSTEMA	예		
		SYSTEMB	예		
		SYSTEMC	예		

계정 관리 보고서

표준 계정 관리 보고서는 사용자 계정의 개요를 제공합니다.

참고: 보고서 제목은 BusinessObjects InfoView 에 나타나는 이름입니다.

다음은 표준 계정 관리 보고서의 목록입니다.

CA Access Control 관리자

CA Access Control 관리자 보고서는 CA Access Control 관리 권한이 있는 모든 사용자 목록을 표시합니다. 여기에는 ADMIN, PWMANAGER 또는 OPERATOR 특성이 있는 사용자가 포함됩니다. 이 보고서는 파이형 차트로 요약 데이터를 표시하고 사용자 이름별 상세 목록을 표 형식으로 표시합니다.

CA Access Control 을 관리할 수 있는 사용자가 많으면 기업이 보안 위험에 노출될 수 있습니다. 물론 평가 중인 끝점이 개발 또는 테스트 환경에 있는 경우 시스템의 사용자 대부분이 CA Access Control 관리자가 되는 것은 정상적입니다.

CA Access Control 그룹 사용자 구성원

CA Access Control 그룹 사용자 구성원 보고서에서는 사용자 그룹 및 해당 구성원을 보여줍니다. 이 보고서에는 세부 정보가 표 형식으로 표시됩니다.

관리를 단순화하기 위해 CA Access Control 환경의 각 사용자를 현재 정의된 CA Access Control 그룹 하나 이상의 구성원으로 포함할 수 있습니다. 또한 사용자 정의 이외에 그룹 정의에 따라 리소스 액세스를 허용할 수 있습니다. 따라서 그룹 구성원이 의도되지 않은 리소스에 대한 사용 권한을 부여하지 않도록 그룹 및 해당 구성원을 자세히 검토해야 합니다.

CA Access Control 그룹

CA Access Control 그룹 보고서는 그룹이 있는 정의된 호스트 및 그룹 설명뿐만 아니라 중첩 그룹으로 알려진 자식 그룹이 포함되어 있는지 여부를 표시합니다.

기업 전체에서 어떤 호스트에 어떤 그룹이 있는지 파악하면 관리 작업을 수행할 때 유용합니다. 또한 다른 그룹이 포함된 그룹을 알고 있으면 특정 사용자나 그룹이 특정 리소스에 액세스할 수 있는 이유를 확인하는 데 유용합니다.

CA Access Control 비활성 기간

CA Access Control 비활성 기간 보고서는 지정된 기간(예: 90 일) 동안 로그온하지 않은 사용자를 표시합니다. 또한 해당 사용자가 일시 중단되어 있는지 또는 시스템에 계속 액세스할 수 있는지 여부를 표시합니다. 이 보고서에는 계정이 비활성 상태이고 일시 중단된 사용자와 계정이 비활성 상태이지만 일시 중단되지 않은 사용자를 비교해서 나타낸 요약 원형 차트가 포함되어 있습니다.

모든 엔터프라이즈 환경에서 감사의 주안점은 어떤 사용자가 현재 환경에 액세스할 수 있는지와 마지막으로 액세스한 시간을 파악하는 데 있습니다. 예를 들어 사용자가 마지막으로 리소스에 액세스하여 끝점에 로그인한 시간뿐 아니라 계정이 비활성 상태로 지속된 기간을 표시해야 합니다. 이 보고서는 서비스 계정의 액세스 규칙성을 증명하고 계속 열려 있지만 특정 기간 동안 액세스하지 않은 계정을 식별하는 데 유용합니다.

CA Access Control 암호 변경

CA Access Control 암호 변경 보고서는 지정된 기간 내에 암호를 변경해야 하는 사용자 계정 목록을 표시합니다. 이 보고서에는 암호를 변경할 필요가 없는 사용자 계정, 암호를 업데이트해야 하는 사용자 계정 및 암호가 만료된 사용자 계정의 요약 파이형 차트가 제공됩니다. 또한 호스트 ID 및 사용자 계정의 암호가 만료될 때까지 남은 날짜 같은 세부 정보가 제공됩니다.

유효하지 않은 암호의 상태를 파악하는 것과 유사한 감사 요구 사항은 암호 변경을 보류 중인 사용자 목록을 파악하기 위한 요구 사항입니다. 파악한 정보를 사용하여 곧 무효화될 수 있는 계정에서 보류 중인 보안 노출을 확인할 수 있습니다.

CA Access Control 암호 만료

CA Access Control 암호 만료 보고서는 지정된 일 수 내에 암호를 업데이트하지 않은 사용자 계정을 표시합니다. 이 보고서에는 암호를 업데이트한 사용자 계정, 암호가 만료되어 시스템 액세스가 일시 중단된 사용자 계정 및 암호가 만료되었지만 시스템에 계속 액세스할 수 있는 사용자 계정을 식별하는 요약 파이형 차트가 제공됩니다. 또한 호스트 ID를 포함하여 지난 x 일 내에 암호를 변경하지 않은 사용자 계정에 대한 세부 정보, 마지막 암호 변경 날짜 및 사용자 계정이 시스템에 계속 액세스할 수 있는 이유가 제공됩니다.

CA Access Control 에는 추가적인 품질 확인 기능을 제공하고 이전 암호 기록을 유지하여 빈번한 재사용을 방지함으로써 끝점 암호 보안을 향상할 수 있는 기능이 있습니다. 이 구성 요소의 일부로 마지막 암호 변경 날짜가 유지됩니다. CA Access Control 은 암호 품질 모델의 이 구성 요소를 사용하여 기업에서 지정된 기간 내에 암호를 변경하지 않은 사용자를 식별할 수 있습니다. 이 보고서가 특히 중요한 이유는 이 보고서를 사용하여 엔터프라이즈 로그인 환경에서 유효하지 않은 암호로 인해 발생할 수 있는 취약점을 중앙에서 확인할 수 있다는 것입니다.

CA Access Control 암호 정책 준수(계정)

CA Access Control 암호 정책 준수(계정) 보고서는 암호 정책(예: 암호 길이와 최소 숫자 및 영문자 수)에 맞지 않는 암호를 가진 사용자 계정을 표시합니다. 이 보고서에는 정책에 맞는 사용자 계정 수와 정책에 맞지 않는 사용자 계정 수를 식별하는 요약 파이형 차트가 제공됩니다. 또한 정책이 적용되지 않는 사용자 계정에 대한 세부 정보가 표 형식으로 제공됩니다.

CA Access Control 암호 정책 준수(호스트)

CA Access Control 암호 정책 준수(호스트) 보고서는 사용자 계정의 암호 정책(예: 암호 길이와 최소 숫자 및 영문자 수)에 맞지 않는 암호를 가진 호스트를 표시합니다. 이 보고서에는 정책에 맞는 호스트 수와 정책에 맞지 않는 호스트 수를 식별하는 요약 파이형 차트가 제공됩니다. 또한 정책이 적용되지 않는 호스트와 해당 호스트에 있는 사용자 계정에 대한 세부 정보가 표 형식으로 제공됩니다.

CA Access Control 권한 분리

CA Access Control 권한 분리 보고서는 권한 분리 정책(예: 사용자가 관리자 사용자 그룹과 감사자 사용자 그룹 모두의 구성원이 될 수 없음)을 위반하는 사용자 계정을 표시합니다. 이 보고서에는 정책에 맞는 사용자 수와 맞지 않는 사용자 수를 비교하는 요약 파이형 차트가 제공됩니다. 또한 정책과 호스트 ID 에 맞지 않는 사용자 계정에 대한 세부 정보가 포함되어 있습니다.

모든 엔터프라이즈 환경의 모든 끝점은 OS 와 응용 프로그램 구성 요소에 액세스할 수 있는 사용자가 유지 관리해야 합니다. 일반적으로 시스템 관리자는 OS 관점에서 컴퓨터를 유지 관리하고 응용 프로그램 관리자는 응용 프로그램 관점에서 컴퓨터를 유지 관리합니다. 예를 들어 Solaris 시스템 관리자는 UNIX 호스트 파일의 항목을 업데이트하고 Oracle DBA 는 Oracle 데이터베이스의 테이블을 유지 관리할 수 있습니다.

이 모델의 장점은 시스템 관리자와 응용 프로그램 관리자가 각각 응용 프로그램의 가용성과 OS 의 가용성을 조정하는 데 제한이 있다는 것입니다. 일반적으로 시스템 관리자가 응용 프로그램 관리자 역할까지 수행하는 것은 바람직하지 않습니다.

이 보고서는 두 그룹에 모두 속한 사용자를 식별하여 역할 범위가 제대로 지정되지 않은 사용자를 식별하는 데 도움을 줍니다. 두 그룹의 공통 부분을 검색하고 보고하는 것은 ISO7799, SOX, PCI, HIPAA 및 DoD 에 대한 주요 감사 항목 중 하나를 충족하는 데 매우 유용합니다.

CA Access Control 사용자 그룹 구성원

CA Access Control 사용자 그룹 구성원 보고서는 배포에서 각 호스트에 대한 사용자 및 사용자가 속한 사용자 그룹을 표시합니다. 이 보고서에는 사용자 및 사용자가 속한 그룹의 호스트 ID 별로 정렬된 세부 정보가 제공됩니다.

CA Access Control 사용자 생성 날짜

CA Access Control 사용자 생성 날짜 보고서는 배포에서 지정된 호스트 또는 모든 호스트에 대해 특정 기간 내에 생성된 사용자 계정을 표시합니다. 이 보고서에는 사용자 계정이 생성된 날짜에 대한 세부 정보가 호스트 ID 별로 정렬된 후 다시 사용자 계정별로 정렬되어 제공됩니다.

CA Access Control 사용자 중단 날짜

CA Access Control 사용자 중단 날짜 보고서는 배포에서 지정된 호스트 또는 모든 호스트에 대해 특정 기간 내에 일시 중단된 사용자 계정을 표시합니다. 이 보고서에는 사용자 계정이 일시 중단된 날짜에 대한 세부 정보가 호스트 ID 별로 정렬된 후 다시 사용자 계정별로 정렬되어 제공됩니다.

CA Access Control 사용자 업데이트 날짜

CA Access Control 사용자 업데이트 날짜 보고서는 배포에서 지정된 호스트 또는 모든 호스트에 대해 특정 기간 내에 업데이트된 사용자 계정을 표시합니다. 이 보고서에는 사용자 계정이 업데이트된 날짜에 대한 세부 정보가 호스트 ID 별로 정렬된 후 다시 사용자 계정별로 정렬되어 제공됩니다.

권한 보고서

표준 권한 보고서는 사용자 및 리소스 권한의 개요를 제공합니다.

참고: 보고서 제목은 BusinessObjects InfoView 에 나타나는 이름입니다.

표준 권한 보고서의 목록입니다.

CA Access Control 기본 리소스 준수(호스트)(페이지 158)
CA Access Control 그룹 권한(페이지 159)
그룹별 CA Access Control 리소스 액세스(페이지 159)
사용자별 CA Access Control 리소스 액세스(페이지 159)
CA Access Control 사용자 권한(페이지 159)

CA Access Control 기본 리소스 준수(호스트)

CA Access Control 기본 리소스 준수(호스트) 보고서는 지정된 리소스에 대한 기본 설정되지 않은 액세스 권한이 있는 사용자 계정을 표시합니다. 이 보고서에는 기본 설정되지 않은 액세스가 허용된 호스트 수와 기본 설정되지 않은 액세스 권한이 있는 총 사용자 계정 수가 표시된 요약 파이형 차트가 제공됩니다. 기본 설정되지 않은 액세스 권한이 있는 각 사용자 계정의 액세스 권한에 대한 호스트별 세부 정보도 제공됩니다.

CA Access Control 그룹 권한

CA Access Control 그룹 권한 보고서는 사용자 그룹이 액세스할 수 있는 모든 리소스 목록을 표시하며 다음 항목을 확인할 수 있는 리소스 이름별 상세 목록을 표 형식으로 표시합니다.

- 호스트 ID
- 액세스 권한
- 액세스 권한이 기본적으로 부여되는지 또는 프로그램을 사용하여 부여되는지 여부
- 적용 가능한 달력 이름이나 기타 시간 제한 같은 모든 제한
- 리소스를 소유하는 사용자 그룹이기 때문에 액세스 권한이 부여되었는지 여부

이 보고서를 사용하여 기업 전체 또는 특정 호스트에 대해 정의된 리소스에 액세스할 수 있는 사용자 그룹을 확인할 수 있습니다. 검토 후 액세스 권한을 보안 정책에 맞게 변경할 수 있습니다.

그룹별 CA Access Control 리소스 액세스

그룹별 CA Access Control 리소스 액세스 보고서는 지정된 리소스에 대해 사용자 그룹에 부여된 액세스 권한을 표시합니다. 이 보고서에는 호스트 ID, 액세스 권한, 기본 액세스 권한 부여 여부 및 기타 제한 사항(예: 요일 및 시간) 지정 여부를 포함하여 리소스에 액세스할 수 있는 모든 사용자 그룹에 대한 상세 목록이 제공됩니다.

사용자별 CA Access Control 리소스 액세스

사용자별 CA Access Control 리소스 액세스 보고서는 지정된 리소스에 대해 사용자 계정에 부여된 액세스 권한을 표시합니다. 이 보고서에는 호스트 ID, 액세스 권한, 기본 액세스 권한 부여 여부 및 기타 제한 사항(예: 요일 및 시간) 지정 여부를 포함하여 리소스에 액세스할 수 있는 모든 사용자 계정에 대한 자세한 목록이 제공됩니다.

CA Access Control 사용자 권한

CA Access Control 사용자 권한 보고서는 사용자에 대한 액세스 권한을 리소스별로 표시합니다. 사용자가 액세스할 수 있는 각 리소스에 대해 보고서는 사용자의 액세스 유형, 기본 액세스, 사용자가 리소스에 액세스하기 위해 사용할 수 있는 프로그램, 리소스에 대한 사용자의 액세스 시간 제한을 제공합니다. 이 보고서는 또한 사용자가 리소스 소유자인지 여부를 지정합니다.

기타 보고서

표준 기타 보고서는 모니터링되는 파일, 모니터링되는 프로그램, 시스템을 다시 부팅하지 않고 CA Access Control 커널을 언로드하기 위한 UNIX 호스트의 준비 상태에 대한 정보를 제공합니다.

참고: 보고서 제목은 BusinessObjects InfoView 에 나타나는 이름입니다.

다음은 표준 기타 보고서의 목록입니다.

CA Access Control 모니터링되는 파일

CA Access Control 모니터링되는 파일 보고서는 기업 전체에서 호스트의 중요한 시스템 파일 상태를 표시합니다. 이 보고서에는 파일이 모니터링되지 않는 호스트, 파일이 모니터링되지만 수정된 호스트 및 파일이 모니터링되고 트러스트된 상태로 유지되는 호스트를 나타내는 요약 파이형 차트가 제공됩니다. 또한 해당 호스트의 파일에 대한 정책을 검토하거나 권한 있는 사용자가 파일을 수정했는지 여부를 검토할 수 있도록 파일의 세부 정보(예: 호스트 ID)가 제공됩니다.

데이터 무결성을 보호하려면 중요한 시스템 파일을 반드시 모니터링해야 합니다. 파일이 변경된 시간을 파악하면 감사 추적을 통해 권한 있는 사용자가 보안 정책에 따라 변경을 수행했는지 확인할 수 있습니다.

CA Access Control 모니터링되는 프로그램

CA Access Control 모니터링되는 프로그램 보고서는 기업 전체에서 호스트의 중요한 프로그램 상태를 표시합니다. 이 보고서에는 프로그램이 모니터링되지 않는 호스트, 프로그램이 모니터링되지만 수정된 호스트 및 프로그램이 모니터링되고 트러스트된 상태로 유지되는 호스트를 나타내는 요약 파이형 차트가 제공됩니다. 또한 해당 호스트의 프로그램에 대한 정책을 검토하거나 권한 있는 사용자가 프로그램을 수정했는지 여부를 검토할 수 있도록 프로그램의 세부 정보(호스트 ID)가 제공됩니다.

데이터 무결성을 보호하려면 중요한 프로그램을 반드시 모니터링해야 합니다. 프로그램이 변경된 시간을 확인하면 감사 추적을 통해 권한 있는 사용자가 보안 정책에 따라 변경을 수행했는지 확인할 수 있습니다.

언로드 고려 사항이 있는 CA Access Control UNIX 호스트

언로드 고려 사항이 있는 CA Access Control UNIX 호스트 보고서는 CA Access Control 커널의 언로드를 방해하는 차단된 시스템 호출이 있는 UNIX 호스트를 표시합니다. 이러한 호스트에서는 커널을 언로드하고 CA Access Control 을 업그레이드하려면 먼저 컴퓨터를 다시 시작해야 합니다.

이 보고서는 언로드 고려 사항이 있는 각 호스트에 대해 프로세스 및 부모 프로세스 ID, 프로그램 이름, 차단 시간, 임계값 시간을 나열합니다. 이 보고서는 또한 각 시스템 호출이 블로킹 호출인지 여부를 지정합니다.

보고서는 다음 범주로 호스트를 그룹화합니다.

- **준비되지 않음(오버플로)** - 시스템 호출 테이블이 크기를 초과했으며 커널을 언로드하기 위해 재부팅이 필요합니다.
- **준비되지 않음(블로킹 시스템 호출)** - 블로킹하는 차단된 시스템 호출이 있으며 커널을 언로드하기 위해 재부팅이 필요합니다.
- **가능성 높음(비블로킹 시스템 호출)** - 블로킹하지 않는 차단된 시스템 호출이 있으며 커널을 언로드하기 위해 일반적으로 재부팅이 필요하지 않습니다.

CA Access Control UNIX 언로드 준비

CA Access Control UNIX 언로드 준비 보고서는 시스템 재부팅 없이 CA Access Control 커널을 언로드하고 CA Access Control 을 업그레이드하기 위한 UNIX 호스트의 준비 상태를 표시합니다.

이 보고서는 커널을 언로드할 준비가 된 호스트, 준비가 되었을 가능성이 높은 호스트, 준비가 되지 않은 호스트의 비율을 원형 차트로 요약 표시합니다. 이 보고서는 또한 각 호스트에 대해 차단된 시스템 호출 및 블로킹하지 않는 시스템 호출의 수를 표시합니다.

보고서는 다음 범주로 호스트를 그룹화합니다.

- **준비되지 않음(오버플로)** - 시스템 호출 테이블이 크기를 초과했으며 커널을 언로드하기 위해 재부팅이 필요합니다.
- **준비되지 않음(블로킹 시스템 호출)** - 블로킹하는 차단된 시스템 호출이 있으며 커널을 언로드하기 위해 재부팅이 필요합니다.
- **가능성 높음(비블로킹 시스템 호출)** - 블로킹하지 않는 차단된 시스템 호출이 있으며 커널을 언로드하기 위해 일반적으로 재부팅이 필요하지 않습니다.
- **준비** - 차단된 시스템 호출이 없으며 커널을 언로드하기 위해 다시 부팅할 필요가 없습니다.
- **해당 없음** - 호스트가 UNIX 호스트가 아닙니다.
- **알 수 없는 상태** - 호스트에 대한 정보가 없습니다.

정책 관리 보고서

표준 정책 관리 보고서는 CA Access Control 엔터프라이즈 관리 정책에 대한 정보를 제공합니다.

참고: 보고서 제목은 BusinessObjects InfoView 에 나타나는 이름입니다.

다음은 표준 정책 관리 보고서의 목록입니다.

CA Access Control 호스트 그룹별 규칙 위반(페이지 166)

CA Access Control 정책 할당

CA Access Control 정책 할당 보고서는 지정된 DMS 에 정의된 호스트 및 호스트 그룹에 배포된 정책의 할당 세부 정보를 표시합니다. 이 보고서에는 다음과 같은 정보가 표시됩니다.

- 정책 이름
- 할당 유형(호스트 또는 호스트 그룹)
- 정책이 배포된 호스트 또는 호스트 그룹의 이름

CA Access Control 정책 배포 스코어카드

CA Access Control 정책 배포 스코어카드 보고서는 지정된 정책에 대한 배포 정보를 표시합니다. 이 보고서는 다음 정보를 원형 차트로 요약하여 표시합니다.

- 정책이 올바르게 배포된 호스트의 수
- 정책이 배포되었지만 오류 또는 위반이 발생한 호스트의 수
- 위험한 상태(정책이 호스트에 할당되었지만 정책이 호스트에 배포되지 않음)인 호스트의 수

이 보고서는 또한 정책 배포에 대한 모든 문제를 호스트별로 자세히 표시합니다.

CA Access Control 호스트별 정책 배포 스코어카드

CA Access Control 호스트별 정책 배포 스코어카드는 정책에 대한 배포 정보를 호스트별로 표시합니다. 이 보고서는 다음 정보를 원형 차트로 요약하여 표시합니다.

- 정책이 올바르게 배포된 호스트의 수
- 정책이 배포되었지만 오류 또는 위반이 발생한 호스트의 수
- 위험한 상태(호스트 또는 호스트가 구성원으로 속해 있는 호스트 그룹에 정책이 할당되었지만 정책이 이 호스트에 배포되지 않음)인 호스트의 수

이 보고서는 또한 정책 배포에 대한 모든 문제를 호스트별로 자세히 표시합니다.

CA Access Control 호스트 그룹별 정책 배포 스코어카드

CA Access Control 호스트 그룹별 정책 배포 스코어카드는 정책에 대한 배포 정보를 호스트 그룹별로 표시합니다. 이 보고서는 다음 정보를 원형 차트로 요약하여 표시합니다.

- 정책이 올바르게 배포된 호스트 그룹의 호스트 수
- 정책이 배포되었지만 오류 또는 위반이 발생한 호스트 그룹의 호스트 수
- 호스트 그룹에서 위험한 상태(정책이 호스트 그룹에 할당되었지만 정책이 호스트에 배포되지 않음)인 호스트 수

이 보고서는 또한 정책 배포에 대한 모든 문제를 호스트 그룹별로 자세히 표시합니다.

CA Access Control 호스트별 정책 배포 상태

CA Access Control 호스트별 정책 배포 상태 보고서는 정책에 대한 상태 정보를 호스트별로 표시합니다. 이 보고서는 다음을 포함한 각 정책의 버전 정보를 제공합니다.

- 위반 상태
- 배포 시간
- 정책을 배포한 사용자의 이름

CA Access Control 호스트 그룹별 정책 배포 상태

CA Access Control 호스트 그룹별 정책 배포 상태 보고서는 정책에 대한 상태 정보를 호스트 그룹별로 표시합니다. 이 보고서는 다음을 포함하여 각 정책의 버전 정보를 제공합니다.

- 위반 상태
- 배포 시간
- 정책을 배포한 사용자의 이름

이 보고서는 또한 정책이 배포된 호스트 그룹 내의 호스트를 나열합니다.

CA Access Control 정책 인벤토리

CA Access Control 정책 인벤토리 보고서는 다음을 포함하여 DMS 에 저장된 정책의 스냅숏을 표시합니다.

- 각 정책이 마지막으로 업데이트된 시간
- 정책을 마지막으로 업데이트한 사용자의 이름
- 정책의 배포된 버전 수
- 정책의 최종 완료된 버전
- 정책이 종속된 다른 정책의 이름

참고: 정책이 다른 정책에 종속된 경우 종속된 상위 정책이 배포될 때까지 정책을 배포할 수 없습니다.

CA Access Control 정책 규칙

CA Access Control 정책 규칙 보고서는 정책에 있는 각 규칙의 배포 및 배포 취소 스크립트를 정책 이름별로 표시합니다. 이 보고서는 규칙이 마지막 업데이트된 날짜와 규칙을 마지막으로 업데이트한 사용자의 이름을 제공합니다. 이 보고서는 또한 정책이 최종 완료되어 배포할 준비가 되었는지 여부를 지정하고 정책 버전 번호를 지정합니다.

CA Access Control 정책 버전

CA Access Control 정책 버전 보고서는 각 정책에 대한 버전 정보를 정책 이름별로 표시합니다. 각 정책에 대해 보고서는 다음 내용을 표시합니다.

- 현재 버전 번호
- 버전이 배포된 날짜
- 현재 버전을 배포한 사용자의 이름

이 보고서는 또한 현재 버전이 최종 완료되었는지 여부도 지정합니다.

CA Access Control 호스트별 규칙 위반

CA Access Control 호스트별 규칙 위반 보고서는 정책 상태 및 규칙 위반을 호스트별로 표시합니다. 이 보고서는 각 호스트에 있는 정책의 목록 및 각 정책의 상태, 버전, 위반 상태를 제공합니다. 정책에 대한 규칙 위반이 있으면 이 보고서는 위반에 대한 세부 정보(즉, 위반이 적용되는 리소스 및 속성에 대한 세부 정보)를 제공합니다.

CA Access Control 호스트 그룹별 규칙 위반

CA Access Control 호스트 그룹별 규칙 위반 보고서는 정책 상태 및 규칙 위반을 호스트 그룹별로 표시합니다. 이 보고서는 각 호스트 그룹에 있는 정책의 목록 및 각 정책의 상태, 버전, 위반 상태를 제공합니다. 정책에 대한 규칙 위반이 있으면 이 보고서는 호스트 그룹에 있는 각 호스트 구성원의 위반에 대한 세부 정보(즉, 위반이 적용되는 리소스 및 속성에 대한 세부 정보)를 제공합니다.

암호 정책 보고서

암호 정책 보고서는 CA Access Control 에 정의된 암호 정책에 대한 정보를 제공합니다.

다음은 표준 암호 정책 보고서의 목록입니다.

CA Access Control 암호 정책별 권한 있는 계정(페이지 166)
CA Access Control PUPM 암호 정책(페이지 167)

CA Access Control 암호 정책별 권한 있는 계정

이 보고서는 시스템에 있는 모든 권한 있는 계정과 각각의 암호 정책을 표시합니다. 이 보고서를 사용하여 암호 정책과 연계할 권한 있는 계정을 결정할 수 있습니다. 이 보고서를 검토한 다음에는 현재 상태가 필요한 조건에 부합하는지, 또는 권한 있는 계정을 다시 할당해야 하는지 결정할 수 있습니다.

이 보고서에는 다음과 같은 정보가 표시됩니다.

- 스냅숏 시간
- 암호 정책 이름
- 끝점 유형 및 이름
- 계정 이름
- 마지막 체크 아웃 날짜
- 마지막 암호 변경

CA Access Control PUPM 암호 정책

이 보고서는 복잡성별로 현재 암호 정책을 표시합니다. 이 보고서를 사용하여 기존 암호 정책의 최소/최대 길이 및 기타 정책 매개 변수가 회사의 보안 표준에 부합하는지 여부를 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 날짜
- 암호 정책 이름 및 설명
- 최대 길이
- 최소 길이
- 암호 정책 매개 변수

권한 있는 계정 관리 보고서

권한 있는 계정 관리 보고서를 사용하면 권한 있는 계정 관리의 세부 정보를 볼 수 있습니다.

다음은 표준 권한 있는 계정 관리 보고서의 목록입니다.

CA Access Control 끝점별 권한 있는 계정(페이지 168)
CA Access Control 사용자별 PUPM 역할 및 권한 있는 계정(페이지 168)
CA Access Control 끝점별 권한 있는 계정 요청(페이지 169)
CA Access Control 승인자별 권한 있는 계정 요청(페이지 169)
CA Access Control 요청자별 권한 있는 계정 요청(페이지 170)
CA Access Control 권한 있는 계정별 PUPM 사용자(페이지 170)
CA Access Control 역할별 PUPM 사용자(페이지 171)

CA Access Control 끝점별 권한 있는 계정

이 보고서는 끝점 유형과 끝점 이름별로 권한 있는 계정의 목록을 표시합니다. 이 보고서를 사용하면 끝점 유형과 이름별로 권한 있는 계정을 볼 수 있습니다. 이 보고서를 검토한 다음에는 각 끝점에 연계된 권한 있는 계정의 수를 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 끝점 유형 및 이름
- 계정 이름
- 마지막 체크 아웃 사용자
- 마지막 체크 아웃
- 마지막 암호 변경

CA Access Control 사용자별 PUPM 역할 및 권한 있는 계정

이 보고서는 사용자 계정별로 권한 있는 액세스 역할 및 권한 있는 계정의 목록을 표시합니다. 이 보고서를 사용하면 연계된 역할 및 사용자 계정별로 권한 있는 계정을 검토할 수 있습니다. 이 보고서를 검토한 다음에는 권한 있는 계정 및 CA Access Control 엔터프라이즈 관리 사용자 계정 모두에 연계된 역할을 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 사용자 ID
- 끝점 시간 및 이름
- 역할 이름 및 설명
- 계정 이름
- 예외
- 마지막 암호 변경

CA Access Control 끝점별 권한 있는 계정 요청

이 보고서는 끝점 유형 및 끝점 이름별로 권한 있는 계정 요청의 목록을 표시합니다. 이 보고서를 사용하여 권한 있는 계정을 체크 아웃하기 위한 요청 및 해당 끝점 유형과 이름을 검토할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 끝점 유형 및 이름
- 계정
- 요청자
- 요청 정당화
- 유효 날짜
- 승인자
- 승인자 설명

CA Access Control 승인자별 권한 있는 계정 요청

이 보고서는 승인자별로 권한 있는 계정 요청의 목록을 표시합니다. 이 보고서를 사용하면 요청을 승인한 사용자별로 권한 있는 계정 요청을 검토할 수 있습니다. 보고서를 검토한 다음에는 승인자 역할을 변경하고, 사용자를 추가로 할당하고, 역할에서 사용자를 제거할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 승인자 사용자 ID
- 끝점 유형 및 이름
- 계정
- 요청자 이름 및 ID
- 요청 정당화
- 유효 날짜
- 승인자 설명

CA Access Control 요청자별 권한 있는 계정 요청

이 보고서는 권한 있는 계정의 암호를 요청한 사용자별로 권한 있는 계정 요청을 표시합니다. 이 보고서를 사용하면 권한 있는 계정을 체크 아웃하기 위한 다른 사용자의 요청을 검토할 수 있습니다. 이 보고서를 검토한 다음에는 체크 아웃 요청 수와 요청한 사용자를 파악할 수 있습니다.

이 보고서는 다음과 같은 정보를 수록합니다.

- 스냅숏 이름
- 승인자 사용자 ID
- 끝점 유형 및 이름
- 계정
- 요청 정당화
- 유효 날짜
- 승인자
- 승인자 설명

CA Access Control 권한 있는 계정별 PUPM 사용자

이 보고서는 끝점 유형, 끝점 이름, 이름별로 권한 있는 계정에 액세스할 수 있는 사용자의 목록을 표시합니다. 이 보고서를 사용하면 사용자가 권한 있는 계정에 액세스하는 방법과 각 권한 있는 계정의 원래 이름 및 끝점 유형을 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 유형
- 끝점 유형 및 이름
- 권한 있는 계정 이름
- 사용자 이름
- 사용자 ID
- 요청

CA Access Control 역할별 PUPM 사용자

이 보고서는 사용자의 목록 및 각각의 연계된 권한 있는 계정 역할을 표시합니다. 이 보고서를 사용하면 사용자가 권한 있는 계정 역할에 연계된 방식과 현재 상태가 회사의 보안 표준에 부합하는지 여부를 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 역할 이름
- 구성원 수
- 사용자 이름
- 사용자 ID
- 전자 메일 주소

UNIX 인증 브로커 보고서

UNAB 보고서는 UNAB 관리 태스크의 세부 정보를 제공합니다.

다음은 표준 UNIX 인증 브로커 보고서의 목록입니다.

CA Access Control 호스트별 UNAB 엔터프라이즈 사용자 액세스

이 보고서는 UNAB 호스트에 액세스한 엔터프라이즈 사용자의 목록을 호스트별로 표시합니다. 이 보고서는 각 호스트에 액세스한 엔터프라이즈 사용자, 이러한 사용자의 마지막 로그인 시도, 호스트에 대한 액세스 권한이 부여된 대상(사용자 또는 그룹)에 대한 정보를 제공합니다. 이 보고서를 검토한 다음에는 엔터프라이즈 사용자의 호스트에 대한 액세스 권한을 변경할 수 있습니다.

CA Access Control 엔터프라이즈 사용자별 호스트에 대한 UNAB 액세스

이 보고서는 UNAB 호스트에 액세스한 엔터프라이즈 사용자의 목록을 사용자별로 표시합니다. 이 보고서는 각 호스트에 액세스한 엔터프라이즈 사용자, 이러한 사용자의 마지막 로그인 시도, 호스트에 대한 액세스 권한이 부여된 대상(사용자 또는 그룹)에 대한 정보를 제공합니다. 이 보고서를 검토한 다음에는 엔터프라이즈 사용자의 호스트에 대한 액세스 권한을 변경할 수 있습니다.

CA Access Control UNAB 엔터프라이즈 사용자

이 보고서는 로컬 호스트에 액세스할 수 있는 엔터프라이즈 사용자의 목록을 표시합니다. 이 보고서는 현재 엔터프라이즈 사용자의 계정, ID, 홈 디렉터리, 셸 유형을 표시합니다. 이 보고서를 검토한 다음 사용자 매개 변수를 변경하고 엔터프라이즈 사용자를 추가 또는 제거할 수 있습니다.

CA Access Control UNAB 엔터프라이즈 사용자 작업

이 보고서는 마이그레이션되거나 부분 마이그레이션된 엔터프라이즈 사용자 계정의 작업 목록을 표시합니다. 이 보고서를 사용하여 UNIX 호스트에 있는 엔터프라이즈 사용자의 작업을 검토할 수 있습니다. 이 보고서를 통해 가장 최근의 성공/실패한 로그인 시도, 사용자에 의한 마지막 성공한 암호 변경 등의 정보를 확인할 수 있습니다.

CA Access Control UNAB 엔터프라이즈 그룹

이 보고서는 엔터프라이즈 그룹의 특성을 표시합니다. 이 보고서는 엔터프라이즈 그룹의 세부 정보(예: 그룹 ID)를 제공합니다.

CA Access Control 호스트별 UNAB 그룹 마이그레이션 상태

이 보고서는 호스트별로 그룹 마이그레이션 프로세스의 상태를 표시합니다. 로컬 호스트의 모든 그룹에 대한 상태를 검토하려면 이 보고서를 사용하십시오. 이 보고서는 그룹의 마이그레이션 상태와 마이그레이션 중 발견된 충돌(예: 충돌하는 이름, ID 등)에 대한 정보를 표시합니다.

CA Access Control 그룹별 UNAB 그룹 마이그레이션 상태

이 보고서는 그룹별로 그룹 마이그레이션 프로세스의 상태를 표시합니다. Active Directory 로 마이그레이션하도록 선택한 그룹의 마이그레이션 상태를 보려면 이 보고서를 사용하십시오.

CA Access Control 호스트 그룹별 UNAB 호스트

이 보고서는 호스트 그룹별로 UNAB 호스트 그룹을 표시합니다. 이 보고서를 사용하여 현재 그룹화된 UNAB 호스트의 개요를 볼 수 있습니다.

이 보고서는 다음 매개 변수를 포함합니다.

- 호스트 그룹
- 호스트 이름
- 총 수

CA Access Control UNAB 로컬 그룹 마이그레이션 상태

이 보고서는 모든 로컬 그룹에 대한 마이그레이션 프로세스의 상태를 표시합니다. 이 보고서를 사용하여 모든 호스트에서 마이그레이션 프로세스의 현재 상태를 검토할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 호스트 이름
- 마이그레이션 상태
- 그룹 이름
- 그룹 ID
- 이름 충돌
- GID 충돌
- 구성원 충돌
- Active Directory 그룹 충돌 없음
- 항목 수

CA Access Control UNAB 로컬 그룹 요약

이 보고서는 로컬 그룹 매개 변수의 요약을 표시합니다. 이 보고서를 사용하여 각 UNAB 호스트에서 동일한 그룹의 인스턴스 수를 파악할 수 있습니다. 이 보고서를 검토한 이후에 그룹 매개 변수를 수정할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 호스트 수
- 그룹 이름
- 그룹 ID
- 인스턴스 수

CA Access Control UNAB 로컬 사용자

이 보고서는 사용자 마이그레이션 프로세스의 상태를 표시합니다. 이 보고서는 사용자의 마이그레이션 상태, 로컬 및 Active Directory 특성, 기타 정보를 표시합니다. 이 보고서를 검토하면 모든 호스트에 대한 마이그레이션 프로세스 상태를 파악하고 마이그레이션 프로세스 중에 식별된 충돌을 해결할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 호스트 이름
- 마이그레이션 상태
- 로컬 사용자 이름
- 로컬 사용자 ID
- 엔터프라이즈 사용자 ID
- 주 로컬 그룹 ID
- 주 엔터프라이즈 그룹 ID
- 로컬 홈 디렉터리
- Active Directory 홈 디렉터리
- 로컬 로그인 셸
- Active Directory 로그인 셸
- 로컬 GECOS
- 그룹 충돌
- 항목 수

CA Access Control UNAB 로컬 사용자 요약

이 보고서는 로컬 사용자 매개 변수의 요약을 표시합니다. 이 보고서 안의 정보는 하나의 사용자 계정이 UNIX 호스트에 표시되는 인스턴스의 수를 표시합니다.

이 보고서는 다음 정보를 표시합니다.

- 호스트 수
- 사용자 이름
- 사용자 ID
- 그룹 ID
- 홈 디렉터리
- 로그인 셸
- 항목 수

CA Access Control UNAB 비표준 로컬 사용자

이 보고서는 엔터프라이즈 사용자 계정 특성과 일치하지 않는 특성을 가진 로컬 사용자를 사용자별로 표시합니다. 이 보고서를 사용하면 마이그레이션 프로세스 중 발견된 로컬 사용자 특성과 엔터프라이즈 계정 속성 사이의 차이를 검사하여 수정할 수 있습니다. 이 보고서는 이 계정이 원래 있었던 모든 호스트에 표시되는 대로 사용자 계정 정보를 표시하고 발견된 차이를 강조 표시합니다.

이 보고서는 다음 정보를 표시합니다.

- 사용자 이름
- Hostname
- 사용자 ID
- 그룹 ID
- 홈 디렉터리
- 로그인 셸

CA Access Control UNAB 비표준 로컬 그룹

이 보고서는 엔터프라이즈 그룹 특성과 일치하지 않는 로컬 그룹 특성을 표시합니다. 이 보고서를 사용하면 마이그레이션 프로세스 중 발견된 로컬 그룹 특성과 엔터프라이즈 그룹 속성 사이의 차이를 검사하여 수정할 수 있습니다. 이 보고서는 이 그룹이 원래 있었던 모든 호스트에 표시되는 대로 로컬 그룹을 표시하고 발견된 차이를 강조 표시합니다.

이 보고서는 다음 정보를 표시합니다.

- 그룹 이름
- 호스트 이름
- 그룹 ID

CA Access Control 호스트별 UNAB 사용자 액세스

이 보고서는 UNIX 호스트에 액세스할 수 있는 엔터프라이즈 사용자의 목록을 호스트별로 표시합니다. 이 보고서를 사용하면 호스트에 액세스할 수 있거나 액세스할 수 없는 사용자별로 각 호스트를 검토하고 최근에 성공 또는 실패한 로그인 및 기타 요약 정보를 볼 수 있습니다. 이 보고서에 있는 정보를 검토한 다음에는 호스트에 액세스할 수 있는 사용자를 변경할 수 있습니다.

참고: 이 보고서는 호스트에 대해 기본적으로 액세스 권한이 있는 사용자를 표시하지 않습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 호스트 이름
- 호스트 그룹
- 사용자 이름
- 사용자 그룹
- 액세스
- 성공한 로그인 없음
- 마지막 실패한 로그인
- 마지막 실패한 로그인 시도
- 규칙 원본
- 계정 수

CA Access Control 호스트별 UNAB 사용자 마이그레이션 상태

이 보고서는 호스트별로 로컬 사용자 마이그레이션 상태를 표시합니다. 이 보고서를 사용하면 마이그레이션하도록 선택한 각 사용자의 상태를 볼 수 있습니다. 이 보고서는 사용자 마이그레이션 상태(완전히 마이그레이션됨, 로컬에 보존됨, 부분 마이그레이션됨, 마이그레이션되지 않음)와 마이그레이션 프로세스 중 발견된 충돌을 표시합니다.

이 보고서는 다음 정보를 표시합니다.

- 호스트 이름
- 로컬 사용자 이름
- 다음에 매핑됨:
- 마이그레이션 상태
- 충돌
- 총 수

CA Access Control 사용자별 UNAB 사용자 마이그레이션 상태

이 보고서는 사용자별로 로컬 사용자의 마이그레이션 상태를 표시합니다. 이 보고서를 사용하면 마이그레이션하도록 선택한 각 사용자의 상태를 볼 수 있습니다. 이 보고서는 이 계정이 있었던 호스트의 목록, 마이그레이션 상태(완전히 마이그레이션됨, 로컬에 보존됨, 부분 마이그레이션됨, 마이그레이션되지 않음), 마이그레이션 프로세스 중 발견된 모든 충돌을 표시합니다.

이 보고서는 다음 정보를 표시합니다.

- 로컬 사용자 이름
- 호스트 이름
- 다음에 매핑됨:
- 마이그레이션 상태
- 충돌
- 총 수

CA Enterprise Log Manager 보고서

CA Enterprise Log Manager 보고서는 CA Access Control 및 UNAB 계정 작업, 리소스 관리 등에 대한 자세한 정보를 표시합니다.

CA Enterprise Log Manager 보고서에 대한 자세한 내용은 CA Enterprise Log Manager 설명서를 참조하십시오.

BusinessObjects InfoView 보고서 포털

보고서 포털은 CA Access Control 보고서를 제공하는 응용 프로그램 서버입니다. 이 서버는 BusinessObjects InfoView 포털을 사용하므로 사용자가 중앙 데이터베이스에 저장된 보고 정보를 활용할 수 있습니다.

보고서 작업을 위해 InfoView 열기

BusinessObjects InfoView 를 사용하여 CA Access Control 보고서에 액세스합니다. 다음 절차에서는 보고 인터페이스(BusinessObjects InfoView)에 액세스하는 방법에 대해 설명합니다.

보고서 작업을 위해 InfoView 를 열려면

1. 다음 방법 중 하나를 사용하여 InfoView 를 시작합니다.
   - BusinessObjects InfoView 가 설치된 컴퓨터에서 "시작", "프로그램", "BusinessObjects XI Release 2", "BusinessObjects Enterprise", "BusinessObjects Enterprise Java InfoView"를 차례로 선택합니다.
   - 컴퓨터의 브라우저에서 다음 URL 로 이동합니다.

     `http://ACRPTGUI_host:ACRPTGUI_port/businessobjects/enterprise115`

     ACRPTGUI_host - InfoView 가 설치된 컴퓨터의 이름 또는 IP 주소(보고서 포털).

     ACRPTGUI_port - InfoView 에 액세스하는 데 사용되는 포트 번호(기본값 9085).

   InfoView 로그온 페이지가 나타납니다.
2. InfoView 를 설치할 때 설정한 자격 증명을 입력하고 "로그온"을 클릭합니다.

   InfoView 홈 페이지가 나타납니다.

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서를 참조하십시오.

보고서 실행

보고 인터페이스(BusinessObjects InfoView)를 연 후 보고서를 선택하고 실행할 수 있습니다.

보고서를 실행하려면

1. InfoView 를 엽니다.

   InfoView 홈 페이지가 나타납니다.

2. "홈", "공용 폴더", "CA Reports(CA 보고서)"를 확장하고 왼쪽 프레임에서 CA Access Control 을 클릭합니다.

   CA Access Control 페이지가 나타납니다.

3. 표시할 보고서의 링크 제목을 클릭합니다.

   추가 값을 입력하여 표시할 보고서의 범위를 정의할 수 있는 보고서 페이지가 나타납니다.

4. 양식 필드를 입력하여 가져오려는 보고서 범위를 정의하고 "확인"을 클릭합니다.

   보고서 출력 페이지가 나타납니다.

   추가 쿼리를 수행하여 보고서 생성에 영향을 줄 수 있습니다. 예를 들어 모두 포함하도록 선택하거나 호스트를 선택하여 알려진 모든 호스트 또는 단일 호스트에서 보고서를 생성할 수 있습니다. 또한 과거의 모든 데이터를 표시하거나 특정 날짜 범위의 데이터만 표시하도록 날짜 범위를 지정할 수 있습니다.

   참고: %(퍼센트) 기호를 사용하여 와일드카드 값을 지정할 수 있습니다. %는 표준 SQL 선택 표기법에 따라 사용하며 일반적으로 와일드카드 지정에서 수행하는 것처럼 단일 문자를 나타내지 않습니다.

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서를 참조하십시오.

보고서 예약

다양한 방법으로 보고서를 실행할 수 있습니다. 보고서 제목을 클릭하고 값을 지정하여 보고서를 실행하거나 다양한 옵션을 선택하여 보고서를 예약할 수 있습니다.

보고서를 예약하려면

1. InfoView 를 엽니다.

   InfoView 홈 페이지가 나타납니다.

2. "홈", "공용 폴더", "CA Reports(CA 보고서)"를 확장하고 왼쪽 프레임에서 CA Access Control 을 클릭합니다.

   CA Access Control 페이지가 나타납니다.

3. 예약할 보고서의 제목 아래에서 "일정"을 클릭합니다.

   선택한 보고서의 "일정" 페이지가 나타납니다.

4. "Run object(개체 실행)" 드롭다운 목록 선택을 수정하여 예약된 보고서를 실행할 시간을 지정합니다.

5. "매개 변수" 섹션을 확장하여 보고서 실행에 대해 값을 지정합니다.

   a. "비어 있음"을 클릭하여 각 매개 변수에 대해 값을 정의합니다.

      "Enter prompt values(프롬프트 값 입력)" 섹션 필드가 나타납니다.

   b. 필요에 따라 값을 정의하고 "확인"을 클릭합니다.

      보고서 실행에 사용할 수 있도록 정의한 값이 저장됩니다.

6. "일정"을 클릭하여 선택한 일정 옵션에 따라 보고서를 실행합니다.

   설정한 보고서 일정 인스턴스를 확인하는 "기록" 페이지가 나타납니다.

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서를 참조하십시오.

생성된 보고서 보기

보고서가 생성된 후 CA Access Control 보고서 목록에서 다음 중 하나를 수행하여 보고서를 표시할 수 있습니다.

- 표시할 보고서의 "View Latest Instance(최신 인스턴스 보기)"를 클릭합니다.
- "기록"을 클릭한 다음 날짜와 시간을 클릭하여 표시할 보고서 인스턴스를 선택합니다.

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서를 참조하십시오.

보고서 상태 보기

보고서의 상태를 확인하여 보고서가 성공적으로 실행되었는지 여부를 확인할 수 있습니다.

보고서 상태를 보려면

1. InfoView 를 엽니다.

   InfoView 홈 페이지가 나타납니다.

2. "홈", "공용 폴더", "CA Reports(CA 보고서)"를 확장하고 왼쪽 프레임에서 CA Access Control 을 클릭합니다.

   CA Access Control 페이지가 나타납니다.

3. 표시할 보고서의 "기록" 링크를 클릭합니다.

   보고서가 실행된 날짜 및 시간 목록을 볼 수 있는 보고서의 "기록" 페이지가 나타납니다.

   목록의 각 항목에 다음 내용이 표시됩니다.

   - 인스턴스 시간 - 보고서가 실행된 날짜 및 시간
   - 제목 - 보고서 제목
   - 실행한 사람 - 보고서를 실행한 사용자 이름
   - 매개 변수 - 해당 보고서 실행을 위해 선택한 매개 변수
   - 형식 - 보고서의 출력 형식
   - 상태 - 보고서의 현재 상태(예: 성공)
   - 다시 예약 - 보고서를 다시 실행할 수 있는 링크

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서를 참조하십시오.

사용자 지정 보고서

CA Access Control 보고서는 모두 Crystal Reports Designer XI를 사용하여 작성되었습니다. 그런 다음 BusinessObjects InfoView 를 통해 웹 기반 형식으로 제공됩니다. 제공된 보고서를 사용자 지정하려면 Crystal Reports Designer XI 가 설치되어 있어야 합니다.

참고: 이 안내서의 지침은 처음으로 보고서를 사용자 지정할 때 도움이 되는 몇 가지 힌트를 제공합니다. Crystal Reports Designer XI 에 대한 자세한 내용은 BusinessObjects Enterprise XI Release 2 디자이너 안내서를 참조하십시오.

BusinessObjects 용 CA Access Control Universe

BusinessObjects 용 CA Access Control Universe 는 CA Access Control 보고 서비스 중앙 데이터베이스를 간단하게 표시합니다. Universe 는 데이터베이스의 데이터에 매핑되는 의미 체계 계층입니다. 이 계층은 최종 사용자를 복잡한 데이터베이스 구조에서 분리합니다. Universe 는 클래스 및 개체 집합입니다.

Universe 는 BusinessObjects Enterprise Designer 를 사용하여 작성됩니다. CA Access Control Universe 는 CA 에서 제공되며 이를 통해 CA Access Control 보고 서비스 중앙 데이터베이스에서 간단하게 보고서를 작성할 수 있습니다. CA 에서 개발한 CA Access Control Universe 를 수정하면 안 됩니다. 필요한 경우 자체 universe 를 위한 기반으로 사본을 작성할 수 있습니다.

CA Access Control Universe 보기

BusinessObjects Designer 를 사용하여 CA Access Control Universe 를 볼 수 있습니다.

CA Access Control Universe 를 보려면

1. "시작", "프로그램", "BusinessObjects XI Release 2", "BusinessObjects Enterprise", "Designer"를 차례로 선택합니다.

   BusinessObjects Designer 에 로그인할 수 있는 "User Identification(사용자 ID)" 대화 상자가 나타납니다.

2. 자격 증명을 입력하고 "OK(확인)"를 클릭합니다.

   "Quick Design(빠른 디자인)" 마법사의 시작 화면이 나타납니다.

3. "Run this Wizard at Startup(시작 시 이 마법사 실행)" 확인란의 선택을 취소하고 "Cancel(취소)"을 클릭합니다.

   비어 있는 디자이너 세션이 열립니다. 사용자 이름과 리포지토리 이름이 제목 표시줄에 나타납니다.

4. "파일", "열기"를 클릭하고 CA Access Control Universe 가 포함된 디렉터리로 이동하여 CA Access Control.unv 파일을 선택하고 "열기"를 클릭합니다.

   CA Access Control Universe 가 현재 디자이너 창에서 열립니다.

   참고: CA Access Control Universe 는 기본 universe 파일 저장소로 지정된 디렉터리의 CA Universe\CA Access Control 에 저장됩니다.

표준 보고서 사용자 지정

모든 표준 보고서를 사용자 지정할 수 있습니다. 예를 들어 필요에 따라 제목, 색상, 로고 및 글꼴을 변경할 수 있습니다. 내용을 변경하려면 Crystal Reports Designer XI 에서 보고서를 열어야 합니다. 모든 보고서에는 해당 .rpt 파일이 있습니다. 이 파일을 열어 보고서를 사용자 지정합니다.

표준 보고서를 사용자 지정하려면

1. 디자이너에서 사용자 지정할 .rpt 파일을 엽니다.

   보고서의 디자인 보기가 나타납니다.

2. 다음 중 하나를 수행하십시오.

   - 보고서 제목을 변경하려면 "파일", "요약 정보"를 클릭하고 "제목" 필드에 제목을 입력합니다.
   - 텍스트를 사용자 지정하려면 디자인 보기에서 원하는 텍스트를 강조 표시하고 두 번 클릭하여 편집합니다.
   - 텍스트 모양을 변경하려면 열린 보고서에서 텍스트를 마우스 오른쪽 버튼으로 클릭하고 "Format text(텍스트 형식 지정)"를 선택하고 원하는 대로 속성을 변경합니다.

3. 사용자 지정 .rpt 파일을 저장합니다.

   새 사용자 지정 보고서가 저장되고 게시할 준비가 완료되었습니다.

사용자 지정 보고서 게시

사용자 지정 보고서는 BusinessObjects InfoView 를 사용하여 게시해야 합니다.

사용자 지정 보고서를 게시하려면

1. BusinessObjects InfoView 를 열고 관리자로 로그인합니다.

   InfoView 홈 페이지가 나타납니다.

2. "새로 만들기", "폴더"를 클릭하고 공용 폴더에서 새 폴더를 만듭니다.

   "새 폴더 만들기" 작업 페이지가 나타납니다.

3. 사용자 지정 보고서 폴더의 이름과 설명을 입력하고 "확인"을 클릭합니다.

   새 폴더가 만들어집니다.

4. "새로 만들기", "Document from local computer(로컬 컴퓨터의 문서)"를 클릭하고 생성한 새 폴더에서 Crystal Report 를 클릭합니다.

   "Add a document from your local computer(로컬 컴퓨터에서 문서 추가)" 작업 페이지가 나타납니다.

5. 사용자 지정된 rpt 파일의 보고서 제목과 경로 이름을 입력하고 "확인"을 클릭합니다.

   사용자 지정 보고서가 게시되며 이제 BusinessObjects InfoView 에서 볼 수 있습니다. 다른 보고서와 마찬가지로 예약도 가능합니다.

제 10 장: 예제 정책 배포

이 장은 아래의 주제를 포함하고 있습니다.

즉시 사용 가능한 예제 정책

CA Access Control 에 포함된 예제 정책은 운영 체제와 응용 프로그램 리소스를 보호하기 위해 권장되는 권한 분리 및 최상의 방법론을 제공합니다. 각 정책은 정책의 용도와 포함된 규칙에 대해 설명하는 주석이 포함된 selang 스크립트입니다.

정책은 CA Access Control 을 사용하여 시스템의 보안을 유지하기 위한 기초를 제공합니다. 조직의 실제 보안 정책 및 환경에 맞게 이 예제 정책을 수정해야 합니다. 예를 들어, 운영 체제 정책은 사용자가 실제 설치한 OS 패키지에 맞아야 합니다. 예제 정책을 기초로 실제 구현할 정책을 만들면 사용자 조직을 위한 정책을 보다 수월하게 만들 수 있습니다.

예제 정책은 다음과 같은 일반적인 응용 프로그램 및 운영 체제용으로 제공됩니다.

- 응용 프로그램:
  - Apache
  - JBoss Application Server
  - CA Access Control 웹 서비스
  - Microsoft SQL Server
  - Oracle Database 10g
- 운영 체제:
  - AIX
  - HP-UX
  - Red Hat Enterprise Linux
  - SuSe Linux Enterprise Server

  - Sun Solaris
  - Windows 2003
- 가상화 시스템:
  - VMware ESX Server
  - Hyper-V
  - Solaris 10 Zones

예제 정책이 저장되는 위치

CA Access Control 은 예제 정책을 다음 디렉터리에 설치합니다.

ACInstallDir/samples/Policies/

ACInstallDir

CA Access Control 이 설치된 디렉터리를 정의합니다.

이 위치에는 다음과 같은 세 개의 하위 디렉터리가 있습니다.

- **Applications** - 응용 프로그램 서버 정책이 들어 있습니다.
- **OS** - 운영 체제 정책이 들어 있습니다.
- **Virtualization** - 가상화 시스템 정책이 들어 있습니다.

CA Access Control 은 정책을 실행하는 selang 스크립트가 수록된 텍스트 파일로 정책을 제공합니다. 또한 각 정책에는 보호 정책을 배포 취소하는 데 사용할 수 있는 일치하는 정책이 있습니다.

예제 정책은 OS_ACTION 과 같은 명명 규칙을 사용합니다.

OS

정책이 설계된 대상 운영 체제를 정의합니다.

ACTION

스크립트가 수행하는 정책 작업을 지정합니다.

값: deploy 및 undeploy

예를 들어, 다음 파일은 Red Hat Enterprise Linux 4.0 에 대한 예제 배포 정책을 수록하고 있습니다: _LINUX40_deploy.txt

참고: 응용 프로그램 정책은 배포 취소 스크립트가 없습니다.

예제 정책 스크립트

각 정책은 정책의 용도와 포함된 규칙에 대해 설명하는 주석이 포함된 selang 스크립트입니다. 예제 정책 스크립트는 모범 사례를 보여주기 위해 작성되었습니다.

- 설명

  예제 정책의 각 섹션에서 달성할 목표를 쉽게 이해할 수 있도록 예제 정책에는 설명이 첨부되어 있습니다.

- 컨테이너

  예제 정책은 관련 리소스를 하나의 컨테이너 리소스로 그룹화합니다. 이 방법을 사용하여 공용 정책은 모든 관련 리소스에 한 번 적용됩니다. 정책 규칙(ACL)은 개별 리소스에 적용할 필요가 없습니다. 예를 들어, 정책은 컨테이너를 사용하여 시스템의 모든 구성 파일을 그룹화할 수 있습니다.

  정책 컨테이너는 POL_container_name 과 같은 명명 규칙을 사용합니다. 이러한 컨테이너는 하위 정책과 같은 역할을 합니다. 예를 들어, OS 예제 정책은 POL_SYS_CONF 컨테이너를 사용하여 OS 구성 파일을 보호합니다.

- 역할

  쉽게 사용자를 관리할 수 있도록 예제 정책은 역할에 ACL 을 적용합니다. 각 역할은 실제 사용자를 추가할 수 있는 CA Access Control 사용자 그룹으로 사용됩니다.

  정책 역할은 ROL_role_name 과 같은 명명 규칙을 사용합니다. 예를 들어, 예제 정책은 기본 제공되는 adm 및 lp 와 같은 시스템 사용자에 대해 ROL_SYSTEM 그룹을 사용합니다. 많은 정책은 이러한 사용자에게 적절한 시스템 운용을 위해 폭넓은 사용 권한을 할당하지만 로그인에 사용할 수 없도록 권한의 사용 기간을 제한합니다.

- 변수

  배포할 때 적용할 변경 내용을 최소화하기 위해 예제 정책은 CA Access Control 변수를 사용합니다. 예제 정책은 기본 제공되는 변수를 사용하여 로컬 호스트에 대한 터미널 규칙과 같은 로컬 시스템 리소스를 보호합니다. 예제 정책은 또한 사용자 정의된 변수를 사용하여 간편하게 정책을 변경할 수 있게 합니다. 예를 들어, 사용자 정의된 변수는 관리 사용자의 홈 디렉터리를 포함할 수 있습니다. 관리 사용자가 다른 홈 디렉터리를 사용하는 경우 이 디렉터리만 한 번 변경하면 영향을 받는 모든 규칙이 자동으로 변경됩니다.

예: 정책 스크립트 주석

Solaris SPARC 9 예제 정책에서 가져온 다음 코드 조각은 예제 정책에 주석을 추가하는 방법을 설명합니다. selang 구문 규칙을 사용할 때 해시 기호(#)로 시작하는 줄은 주석입니다.

```
#
# * 홈 디렉터리 보호 정책 *
# ************************************
#
# 이 정책은 FILE 클래스를 사용하여 각 디렉터리의
# 소유자만 액세스할 수 있도록 중요한 사용자의 홈
# 디렉터리를 보호합니다.
#
# 필수 구성 요소:
#      없음
#
# 규칙:
#      없음
#
# 컨테이너:
#      POL_HOME_DIR       - 중요한 사용자의 홈 디렉터리
#
# 컨테이너 POL_HOME_DIR 정의
# 홈 디렉터리 보호
editres  CONTAINER POL_HOME_DIR audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
comment("AC 예제 - 홈 디렉터리 보호")
authorize CONTAINER POL_HOME_DIR uid(* _undefined)  access(NONE)
editres ACVAR ("HOME_OS_ADMIN") value("/root") type(static)
editusr (<!USER_OS_ADMIN>)
# 특정 FILE 리소스를 정의하고 POL_HOME_DIR 와 연결
editres FILE ("<!HOME_OS_ADMIN>/*") audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
defaccess(NONE) <!POLICY_WARNING_MODE>  comment("AC 예제")
authorize FILE ("<!HOME_OS_ADMIN>/*") uid(<!USER_OS_ADMIN>) access(ALL)
chres CONTAINER POL_HOME_DIR mem+("<!HOME_OS_ADMIN>/*") of_class(FILE)
```

예: 예제 정책의 컨테이너

다음 selang 출력은 POL_SYS_FILES 의 속성을 표시합니다. AIX 예제 정책은 시스템 파일을 보호하는 하위 정책을 포함하고 있습니다.

```
AC> sr container POL_SYS_FILES
컨테이너 'POL_SYS_FILES'의 데이터
------------------------------------------------------------------------
ACL                :
    접근자                  액세스
    ROL_SYSADMIN   (GROUP  ) All
    ROL_SYSTEM     (GROUP  ) All
    *              (USER   ) R, Chdir
    _undefined     (USER   ) R, Chdir
구성원          :
    /boot/*        (FILE   )
    /dev/kmem      (FILE   )
    /dev/mem       (FILE   )
    /dev/port      (FILE   )
감사 모드          : 실패
소유자               : +nobody       (USER   )
작성 시간          : 2008-12-10 10:32
업데이트 시간         : 2008-12-10 10:35
업데이트한 사람          : root          (USER   )
설명              : AC 예제 - OS 시스템 파일 보호
```

예: 예제 정책의 변수

Red Hat Enterprise Linux 5 예제 정책에서 가져온 다음 코드 조각은 예제 정책이 변수를 사용하는 방법을 설명합니다. 이 코드 조각에서 예제 정책은 로컬 호스트 및 관리 사용자 root 의 홈 디렉터리에 대한 가능한 이름을 정의합니다.

```
#
# * AC 변수 정의 *
# ****************************
#
# 이 섹션의 규칙은 정책이 사용하는 변수를 정의합니다.
# 변수:
#    LOCALHOST           : 로컬 호스트의 가능한 이름 목록
#    HOME_OS_ADMIN        : root 의 홈 디렉터리
#    POLICY_WARNING_MODE   : 정책 경로 모드 설정(WARNING 또는 WARNING-으로 설정)
#    POLICY_AUDIT_MODE     : 정책 감사 모드 설정
#    POLICY_DEFACCESS      : 정책 리소스의 defaccess 설정
#
```

```
editres ACVAR ("LOCALHOST") value("localhost") type(static)
editres ACVAR ("LOCALHOST") value+("127.0.0.1")
editres ACVAR ("LOCALHOST") value+("0.0.0.0")
editres ACVAR ("HOME_OS_ADMIN") value("/root") type(static)
editres ACVAR ("POLICY_WARNING_MODE") value("WARNING") type(static)
editres ACVAR ("POLICY_AUDIT_MODE")  value("FAILURE") type(static)
editres ACVAR ("POLICY_DEFACCESS")   value("ALL")    type(static)
```

추가 정보:

사용자 정의된 변수(페이지 81)
기본 제공되는 변수(페이지 83)
변수 사용 지침(페이지 84)
끝점이 변수를 해석하는 방법(페이지 85)

정책 배포

CA Access Control 정책을 배포할 때는 정책이 오류 없이 예상한 대로 배포 및 수행되도록 다음과 같은 일부 일반 단계를 따라야 합니다. 다음 섹션에서는 예제 정책을 배포하기 전 및 후에 수행해야 하는 작업에 대해 설명합니다.

정책 배포를 위한 끝점 준비 방법

정책을 구현하기 전에 정책에 대해 끝점을 준비해야 합니다. 이렇게 하면 나중에 이 정책과 특별히 관련된 문제를 파악할 수 있습니다.

정책 배포를 위해 끝점을 준비하려면

- 운영 체제 또는 응용 프로그램의 신규 설치 사용

  OS 정책에 대해 제조업체에서 제공하는 최신 OS 버전 및 패치를 사용하십시오. 이렇게 하면 수정에 따른 잠재적 손상으로부터 시스템을 보호할 수 있습니다. 정책은 시스템이 고의 또는 사고로 인해 변경되지 않도록 보호하므로 정책을 적용한 다음에는 패치를 적용하고 시스템을 필요한 대로 구성할 수 있습니다. 응용 프로그램에도 동일한 논리가 적용됩니다.

- 권한 분리 적용

  정책 규칙을 검토하여 필요한 경우 규칙을 추가하십시오. 역할, 사용자, 사용자의 관계(역할 구성원 자격)를 정의하는 정책을 새로 만드십시오. 그러면 이 정책을 예제 정책 이전 또는 이후에 배포할 수 있습니다.

  한 사용자에게 너무 많은 권한을 부여하지 않도록 주의하십시오. 예를 들어, 기본적으로 superuser 는 CA Access Control 관리 권한을 제공하는 ROL_AC_ADMIN 에 추가되어 있습니다. 하지만 이 사용자를 그룹에서 제거한 후 대신 보안 관리자를 추가하는 것이 좋습니다.

- 새 CA Access Control 데이터베이스 생성 및 기존 데이터베이스 백업

  정책을 배포하기 전에 새 데이터베이스를 만드십시오. 이렇게 하면 정책 규칙이 충돌하거나 데이터베이스의 기존 규칙이 변경되는 것을 방지할 수 있습니다. 새 데이터베이스를 만들 수 없는 경우 정책을 적용하기 이전 상태로 복원할 수 있도록 데이터베이스를 백업해야 합니다.

- 새 감사 로그 파일 사용

  기존 감사 로그 파일을 백업한 후 먼저 파일을 제거하십시오. 이렇게 하면 CA Access Control 이 새 이벤트를 로깅할 때 새 감사 로그 파일을 만듭니다. 감사 로그 파일이 배포하는 정책에 대한 이벤트만 수록하고 있으므로 이 정책과 관련된 문제를 보다 신속하게 파악할 수 있습니다.

- CA Access Control 사용자 정의된 변수 설정

  미리 설정된 CA Access Control 변수 값("AC 변수 정의" 섹션)을 확인하고, 사용하는 환경에 맞게 조정하고, 필요한 경우 값을 추가 또는 수정하십시오.

단계적으로 정책을 배포하는 방법

정책을 배포할 때 정책이 오류 없이 예상한 대로 배포 및 수행되도록 수행할 수 있는 일부 작업이 있습니다. 정책 배포를 위해 끝점을 준비한 다음에는 단계적으로 정책을 배포하는 것이 좋습니다.

단계적으로 정책을 배포하려면

1. 경고 모드에서 정책을 배포합니다.

   이제 정책이 활성화되었지만 규칙을 시행하지는 않습니다. 그런 다음 감사 로그를 검토하여 원하는 정책을 적용하기 전에 해당 정책 결과를 미리 볼 수 있습니다.

   참고: 기본적으로 예제 정책의 스크립트는 모든 정책 규칙에 대해 경고 모드를 설정합니다.

2. CA Access Control 감사 로그에서 경고 메시지를 검토합니다.

   정책을 배포한 이후에는 정책 규칙이 경고 모드를 사용하는 경우 감사 로그에 모든 정책 위반이 경고로 표시됩니다.

3. 실제 시나리오에서 시스템을 사용하고 감사 로그를 다시 분석합니다.

   컴퓨터에서 일상적인 운영 절차(로그인, 서비스/응용 프로그램 시작/중지 등)를 수행하여 정책을 효과적으로 테스트할 수 있습니다. 그런 다음 감사 로그를 다시 분석하여 새 경고가 나타나는지 확인할 수 있습니다.

4. 필요한 경우 정책을 수정합니다.

   감사 로그에서 얻은 정보를 사용하여 사용하는 환경에서 예상대로 작동하도록 정책을 수정할 수 있습니다.

5. 정책을 활성화하기 위해 경고를 제거합니다.

   정책이 실제 업무 환경에서 규칙을 시행할 준비가 되었다고 확신하면 경고 모드를 제거하여 정책을 활성화할 수 있습니다.

   정책이 이제 시행됩니다.

참고: 정책을 수정하려면 먼저 정책 시행을 비활성화하고(경고 모드 사용) 정책을 수정한 다음 변경 내용이 원하는 대로 작동한다고 확신할 때 정책을 다시 활성화해야 합니다.

추가 정보:

예제 정책 배포(페이지 195)
사용하는 환경에 맞게 예제 정책을 사용자 지정하는 방법(페이지 195)
예제 정책 시행 활성화(페이지 196)

예제 정책 배포

예제 정책은 CA Access Control 변수를 포함하므로 고급 정책 관리 방법을 사용하여 배포해야 합니다.

참고: 예제 정책 파일은 끝점의 selang 에서 직접 실행할 수 없습니다.

CA Access Control 엔터프라이즈 관리를 사용하여 예제 정책을 DMS 에 저장한 다음 필요할 때 여러 끝점에 할당하십시오.

추가 정보:

고급 정책 관리(페이지 52)
정책 생성 및 배포 방법(페이지 65)

사용하는 환경에 맞게 예제 정책을 사용자 지정하는 방법

예제 정책은 사용하는 보안 정책을 위한 기초로서 제공됩니다. 예제 정책을 배포하려면 사용하는 환경에 맞게 사용자 지정해야 합니다.

사용하는 환경에 맞게 예제 정책을 사용자 지정하려면

- CA Access Control 및 시스템 로그 파일을 검토합니다.

  배포 프로세스 중 발생한 경고 또는 오류를 파악하여 적절히 정책을 수정합니다.

- 사용자를 정책 규칙에 조인합니다.

  예제 정책은 권한 부여를 위해 역할을 사용합니다. 조직의 사용자를 이 역할에 할당해야 합니다.

  중요! 정책의 배포를 취소할 때는 만든 사용자 또는 그룹을 삭제하지 마십시오. 삭제하는 경우 동일한 사용자 및 그룹을 사용하는 다른 정책에 있는 접근자 연관 관계 및 ACL 목록의 동작에 영향을 줄 수 있습니다.

- (Windows 에만 해당) 공존 유틸리티 eACoexist.exe 를 실행합니다.

  이 유틸리티는 CA Access Control 과 설치된 다른 프로그램 사이의 충돌을 식별하고, 해당 프로그램에 대한 바이패스를 만들어 이 충돌을 해결합니다.

예제 정책 시행 활성화

기본적으로 예제 정책의 스크립트는 변수를 사용하는 모든 정책 규칙에 대해 경고 모드를 설정합니다. 정책을 배포하면 정책이 활성화되지만 규칙이 시행되지는 않습니다. 정책에 익숙해지고 필요한 대로 정책을 사용자 지정할 수 있게 되면 정책 규칙이 시행되도록 정책을 활성화할 준비가 되었습니다.

예제 정책 시행을 활성화하려면

1. 정책 스크립트를 편집하여 POLICY_WARNING_MODE 변수의 값을 "WARNING-"로 변경합니다.

   변경된 스크립트 규칙은 다음과 같습니다.

   ```
   editres ACVAR ("POLICY_WARNING_MODE") value("WARNING-") type(static)
   ```

   리소스 또는 접근자에 대해 warning-를 설정하는 규칙을 실행하면 CA Access Control 은 해당 리소스 또는 접근자의 경고 모드를 제거합니다.

2. 편집된 정책을 배포합니다.

   정책 시행이 활성화됩니다.

예제 정책 시행 비활성화

기본적으로 예제 정책의 스크립트는 변수를 사용하는 모든 정책 규칙에 대해 경고 모드를 설정합니다. 정책 시행을 활성화할 때 경고 모드를 제거합니다. 정책 시행을 비활성화하려면 경고 모드를 다시 사용해야 합니다.

예제 정책 시행을 비활성화하려면

다음 중 하나를 수행합니다.

- 다음과 같이 정책을 경고 모드로 다시 배포합니다.
  a. 정책 스크립트를 편집하여 POLICY_WARNING_MODE 변수의 값을 "WARNING"으로 변경합니다.

     변경된 스크립트 규칙은 다음과 같습니다.

     ```
     editres ACVAR ("POLICY_WARNING_MODE") value("WARNING-") type(static)
     ```

     리소스 또는 접근자에 대해 warning-를 설정하는 규칙을 실행하면 CA Access Control 은 해당 리소스 또는 접근자의 경고 모드를 제거합니다.
  b. 편집된 정책을 배포합니다.

     정책 시행이 활성화됩니다.

  리소스 또는 접근자에 대해 warning 을 설정하는 규칙을 실행하면 CA Access Control 은 해당 리소스 또는 접근자에 대해 경고 모드를 설정합니다.
- 정책을 검토하여 영향을 받는 클래스를 식별하고 이 클래스에 경고 모드를 설정합니다.

정책 시행이 비활성화됩니다.

예제 정책이 배포된 경우 시스템 유지 관리를 수행하는 방법

언젠가는 시스템을 업그레이드하고 새 응용 프로그램을 설치하는 등의 시스템 유지 관리를 수행해야 합니다. 시스템을 유지 관리할 때는 이 절차 중에 오류가 발생하지 않도록 정책을 비활성화해야 합니다.

예제 정책을 배포한 이후에 시스템 유지 관리를 수행하려면 다음을 수행하십시오.

1. 정책 시행을 비활성화합니다.
2. 유지 관리를 수행합니다.
3. 정책 시행을 활성화합니다.
4. CA Access Control 감사 로그 파일을 검토합니다.

   감사 로그는 유지 관리에 따른 영향을 받은 파일에 대한 경고를 수록하고 있습니다.